PERTINO SETUP & USER MANUAL

This manual illustrates the setup process of the Pertino Cloud Network Engine. It also introduces you to some of the powerful features, applications, and usage of Pertino's Engine, and shows you how to perform some basic networking functions.

More information and detailed usage notes for each of these features are available at support.pertino.com.

Table of Contents

Initial Deployment Instructions

Before getting started, you need to have two computers ready to go. Pertino supports Windows, Mac, and Linux devices and servers. Later in this guide, we'll also show you how to access resources on your Pertino network from iOS and Android mobile devices.

Create your Pertino account

1. Navigate to www.pertino.com
2. Click Sign Up.
3. Select the "Start your 30-day free trial" button.
4. Complete the signup form and select "Start your free trial".

Complete the Setup wizard

1. Name your network.
2. Download and install Pertino on a client computer. This will be the first member of your network.
    a. Navigate to Pertino.com/download for the latest installer
    b. Double click the installer and follow the prompts
    c. When asked for credentials, use the email address and password used earlier in the process.
3. Download and install Pertino on a second computer to act as a server on your network.

Web Management Console: People and Devices

To add users and devices to Pertino networks, use the icons along the bottom of the screen to navigate between various selections.

Figure 1. Web management console icons in the navigation bar.

Each screen offers some shortcuts, such as Icon and List views, to make navigation easier.

Adding Users to your Pertino Network

Once your Pertino network is established, you need to add users so they can access the devices and resources your make available. Users on the Pertino network are identified via email address.

Creating accounts for new users

In most cases, you create Pertino accounts for users when you add them to your network. You have the option of either installing the Pertino software directly on to their devices, or providing instructions for self-install.

1. In the Web Management console, navigate to PeopleView.
2. Click the Add People plus sign (+) to begin adding users.
    a. To add a single user, fill in the fields for First Name, Last Name, and email address:

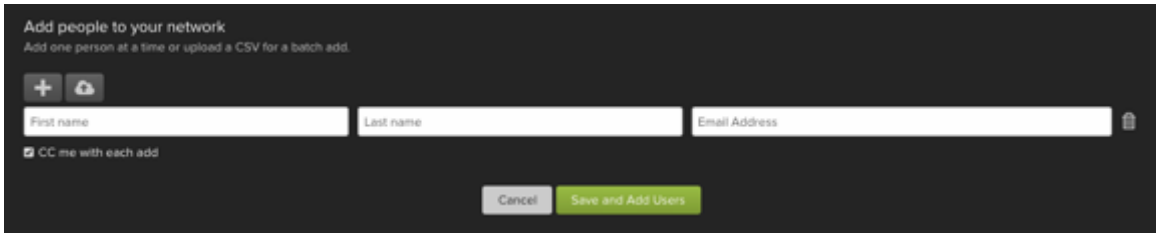


Figure 2. Adding users dialog.

    b. Click the Add People button.
    c. To add multiple users at once, click the upload file within the cloud icon to upload a CSV list of users, one per line.
    d. When you click the "Add People" button, the user's account is created and Pertino sends them an email asking them to create a password.
        i. If you check the "cc me" box, you'll get a copy of the email.
        ii. The account is created immediately and you can begin managing users in the Web Management Console even if they haven't yet set their passwords.

NOTE: If you are installing the Pertino client for your users, you can

use your own credentials during the installation process. There is no need to ask anyone to share a password with you.

e. Once you have installed the software and connected their devices to your network, navigate to DeviceView in the Web Management Console (see below) and select the user's device.
    i. Because you used your credentials to connect, the device will initially be assigned to you.
    ii. Click the Assign Device button and select the appropriate user for that device.
f. If you are going to ask users to self-install the Pertino client, now is the time to do so.
    i. After they set their passwords, they can run the installer on their own machines and connect to your Pertino network.

Adding Devices to your Pertino Network

Device Authentication:

You can also add devices to your network using a "Device Authentication Key" without the need to invite or email other users. The device authentication key is used to authenticate a server instead of a username/password.

1. In the Web Management console, navigate to the Settings page.

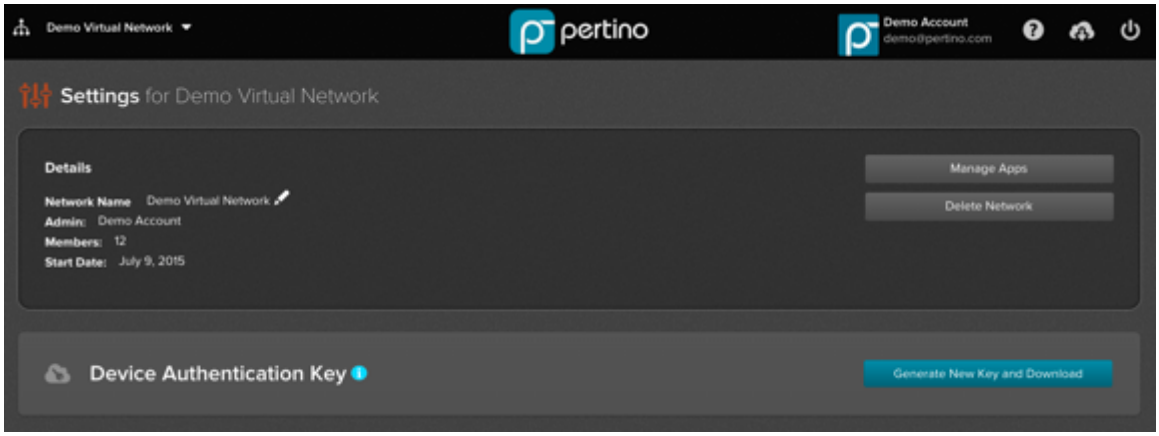


Figure 3. Setting page.

2. Click the "Generate New Key and Download" button.
    a. This will download a file called "apikey.pertino". This single key can be used multiple times which can be useful when deploying Pertino for larger networks.
    b. The installation instructions are below.

NOTE: This key does not expire, but if you want to revoke this key, generating a new key **will** revoke the old key. Devices that used the

old/revoked key will not be impacted. They will remain connected to the network until they are deactivated from the Web Console. When the key is revoked it will not be usable for new device authentications.

This key is specific to the network that is specified when the key was generated. If you need servers to auto-join a different network, navigate to the other network and generate the Device Authentication key.

When you are installing the Pertino client for your servers:

- Windows Server installations instructions using both Windows CMD line and Active Directory's GPO (to deploy Pertino to large numbers of servers) can be found here:

  http://pertino.com/download-windows

- Linux Server installation instructions for both command-line or Puppet/Chef scripts (to deploy Pertino to large numbers of servers can be found here:

  http://pertino.com/download-linux

The server will join the network and can be managed from the web-ui without worrying about passwords expiring or if a user leaves the network/company.

Dashboard

The Dashboard application offers at-a-glance information about the status of your Pertino network. You can determine who is online, what devices they are using, the total number of devices, and the total network usage over the past week.

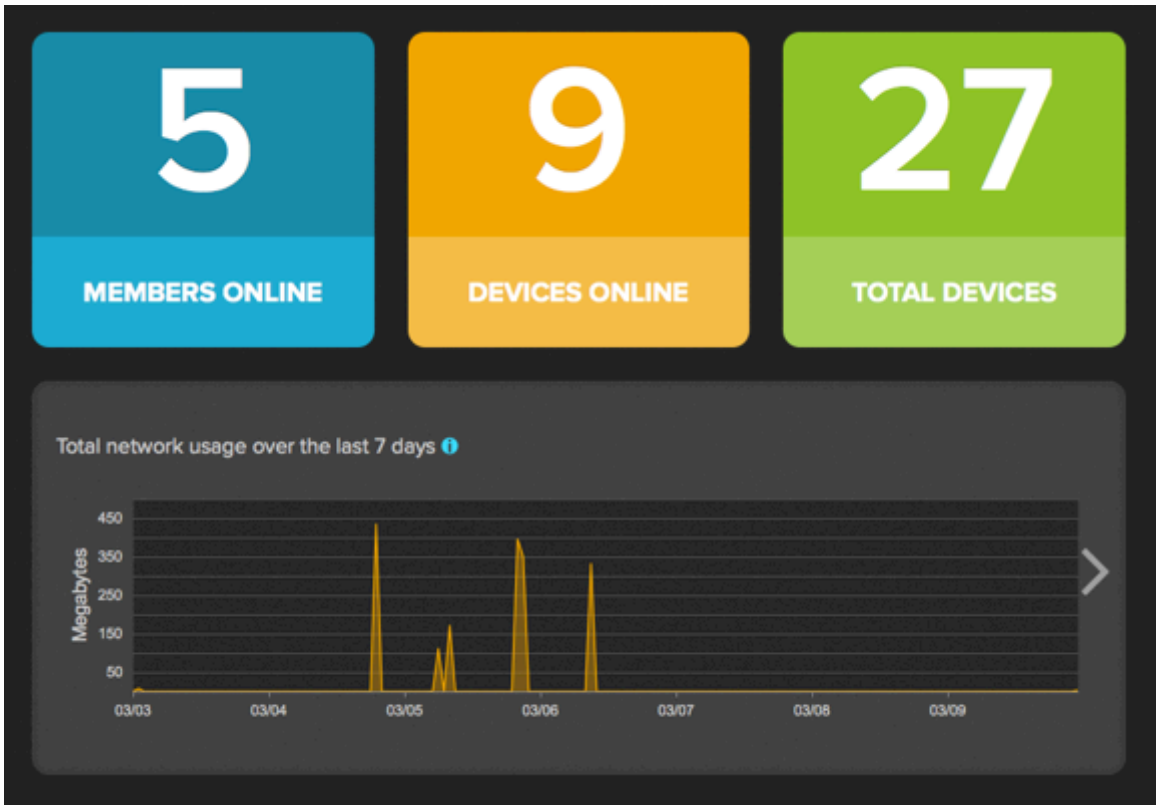


Figure 4. Dashboard application with UsageMonitor enabled.

Search, Icon, and List Views

These buttons are located in the top right corner of the web management console.

- Using the Search field, you can filter the visible items on the page to quickly find a specific user or device.
- Use the Icon and List icons to toggle between views.

Figure 5. Search, Device, and List icons.

- **Icon** view shows a grid of people or devices. Clicking on one of the icons reveals details about that item and any available actions.
- **List** view shows all the people of devices in a table as well as the various attributes of each item. Clicking on the Plus (+) sign next to the item name reveals additional details and action buttons.

Quick Filters

The top row of quick filters allows you to narrow your view to a specific type of item.

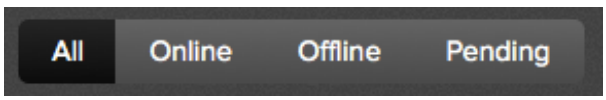


Figure 6. Quick Filters.

PeopleView

PeopleView and DeviceView share similar features. PeopleView allows you to show the people associated with your Pertino network. The Quick Filter options are as follows:

- All—all of the people in your network
- Online
    - A Person is online if at least one of their devices is currently connected to the Pertino network

      NOTE: As a network administrator, you are likely to use your own user credentials when you connect servers to the network. These servers should be designated as "Resources" on the network so that they do not affect your personal online/offline status.

- Offline—a user is offline when none of their devices are connected to the network.
- Pending—a person is "pending" when they have been invited to the network but have not accepted yet.
    - When using the "Add People" button to add users to your network, these users will immediately be added to the network and will initially be displayed as offline.

PeopleView details

- Detailed information about a user can be displayed by clicking on the icon or plus (+) sign.
- You may promote a user from normal privileges to administrative privileges, or you may demote a privileged user to normal privileges.
- You may delete a user from the network.
    - This selection will remove the person from your network, and any associated devices that are currently connected to your network will be disconnected. Any devices that are currently offline will not be able to reconnect to your network when they come back online.

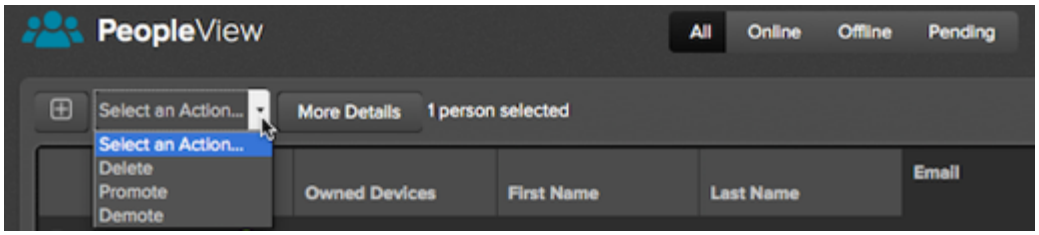


Figure 7. The Detail view icons.

DeviceView

Similarly, the DeviceView panels show the status of the devices associated with your network. The Quick Filter options are as follows:

- All—all of the devices on your network
- Devices—all of the client computers on your network. These are machines associated with the individual users that affect their online/offline status in PeopleView.
- Resources—all of the servers on your network. These are the machines that provide services to your users.
    - They are generally available and connected all the time
    - They are not associated with an individual user and do not affect any user's online/offline status.

DeviceView details

- In both the Icon and List views, detailed information about a user can be displayed by clicking on the icon or plus (+) sign.
- The Detail View also displays the available action buttons.

  NOTE: If you are not the device owner, you will only see the option to "Delete from Network"

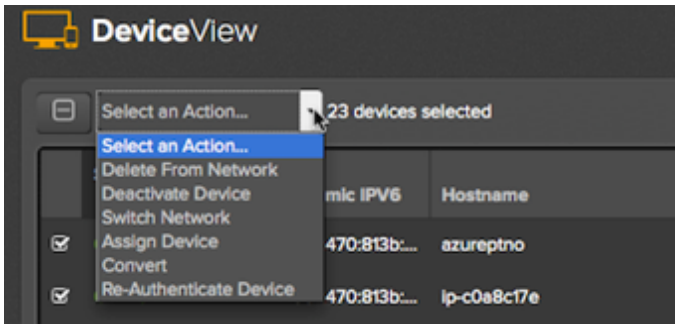


Figure 8. The Device Detail icons.

- Delete From Network—removes the device from the network. It is still eligible to reconnect to any network to which the user has been invited or added. Only appears if you are the owner of the device or the manager of the network to which it is attached.

  NOTE: If you later decide that you want this device to connect to Pertino on any network, you must reinstall the client software. Only appears if you are the owner of the device.

- Deactivate Device—completely deactivates the device from all Pertino networks.

- Switch Network—If the administrator manages multiple Pertino networks, this button allows the device to be moved between networks. Only appears if you are the owner of the device.
- Assign Device—allows the administrator to associate a device with a particular user. Only appears if you are the owner of the device.
- Convert—converts the device to a resource. Only available if it is currently classified as a device.
- Re-Authenticate Device—this option requires a new device authorization or user authorization to join the network.

Getting Started with Pertino Apps

AppScape

AppScape is Pertino's network services App store. Instead of the traditional approach of installing hardware appliances and endpoint software, IT pros can now deploy network services on their Pertino cloud networks with just a few clicks.

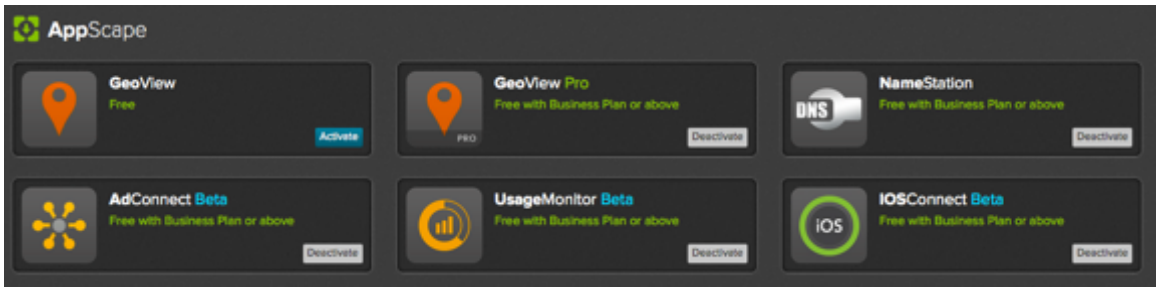


Figure 9. AppScape menu.

Apps are activated and deactivated in the App store.

ADConnect

With ADConnect, you can easily make Active Directory services available to remote users. This app lets you specify which AD Name Servers to use over Pertino so that your remote devices know how to reach your domain controllers. In just three steps, you can provide domain access for remote devices without policy updates, DNS changes, or firewall configuration.

How to setup ADConnect

1. Install Pertino on your Active Directory member servers, including both DNS and application servers.
2. Mark each server as a Resource on your Pertino network. (See the DeviceView section for more information.)
3. Activate the ADConnect app and specify your Name Servers.

Name Servers

DNS is the key to making Active Directory services available to remote clients. When remote clients can use the same DNS servers as computers on your local network, they are able to fully participate in all Active Directory functions including authentication and file access.

How it works

- When ADConnect is enabled, client computers connecting to the Pertino network are instructed to use the specified DNS servers for name resolution.
- Active Directory takes care of all name resolution and replication. Once clients are using AD servers for name resolution, they will get any updates you make to your Active Directory in real time.
- Active Directory DNS servers will make sure clients get the right name resolution depending on their location.
- Local clients (on your private IP address space) will be told to connect locally.
- Remote Pertino clients will be told to connect using Pertino IP address space.

  NOTE: Please see Pertino's support site for a full description of deployment scenarios and caveats.

NameStation

Every device on a Pertino network receives a default DNS name so that other members of the network can access it using the fully qualified domain name (FQDN). NameStation allows the network administrator to choose a custom subdomain and assign aliases to network resources.

Default DNS names

- Each Pertino network is assigned a short subdomain such as "2q1k5f".
- Each device's fully qualified domain name is in the form of hostname.subdomain.pertino.net, so a computer named "Katie-pc" would be **katie-pc.2q1k5f.pertino.net**.

Enabling NameStation

1. Click on the AppScape icon in the bottom navigation bar to visit the store.
   a. NameStation is available for no charge to any Pertino network on a Business Plan or above.
2. Click on the NameStation icon in the store to see a description of the app.
3. Click on the Activate button to turn on NameStation.

Using NameStation

1. Click on the MyApps icon in the bottom navigation bar.
2. Click on the NameStation icon.

3. At the top of the app, click on Customize to create your own subdomain.
    a. Now you can change "2q1k5f" to something more memorable like "acmecorp".

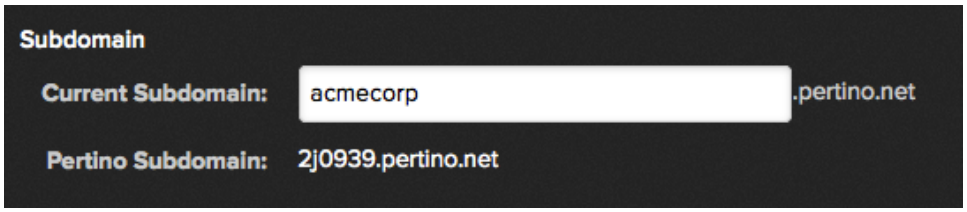


Figure 10. Customize your subdomain.

4. Once you have claimed a custom subdomain, devices on your network can be accessed at the new DNS names. In the example above, the new name for Katie's PC would be **katie-pc.acmecorp.pertino.net**.

Adding alternate names to servers

For computers designated as Resources on your network, you have the option of adding additional DNS names or aliases. For example, you may have a server that is used for both an intranet site and as file server on your network.

- If its hostname is "server3", it would be accessible at **server3.acmecorp.pertino.net**.
- You could add two alternate names of "files" and "intranet" to make access easier for your users. Now, **files.acmecorp.pertino.net** and **intranet.acmecorp.pertino.net** both point to your server.

NetworkView

The NetworkView app enables you to specify a SmartZone or enable a Pertino Gateway. The Pertino Gateway is available only to customers on an Enterprise plan.

The NetworkView app is displayed at the bottom of the **app.pertino.com** page.

Figure 11. NetworkView app icon.

SmartZone

A SmartZone enables a client on a Pertino network to achieve optimal traffic paths through a local network if a local network is available. In other words, SmartZones are designed for remote users who occasionally come into central or branch offices from time to time and don't want network traffic to traverse the Pertino network when there is a local—and possibly better performing—network.

NOTE: Once you add a SmartZone and then save it, clients will be provisioned with their SmartZone membership immediately.

Only network administrators can configure SmartZones. The following procedures illustrate the process.

Creating SmartZones

1. Select "NetworkView".
    a. A "SmartZones" splash screen displays.

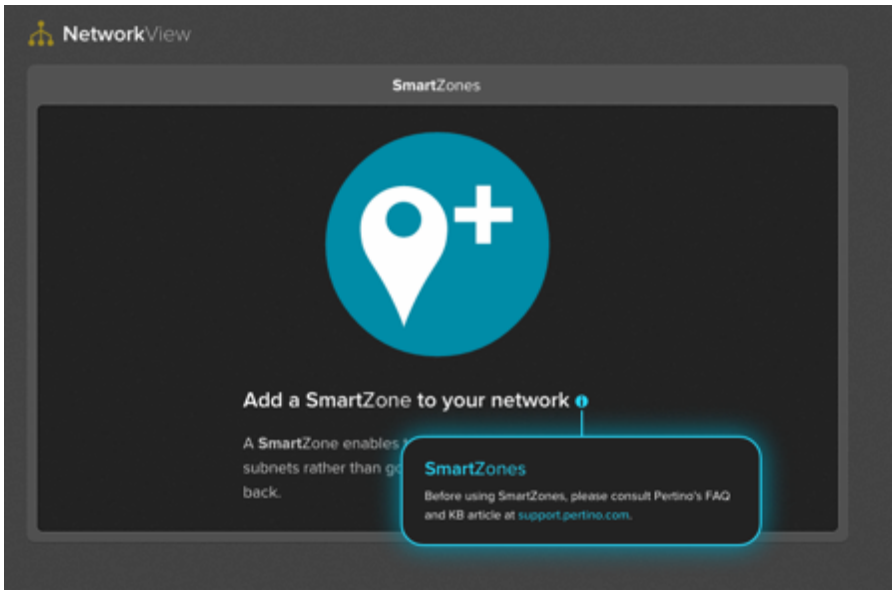


Figure 12. SmartZone splash screen.

2. Select the large "Add Zone" icon in the middle of the splash screen.
    a. **NOTE**: this splash screen only displays upon the first instance of creating a SmartZone. Subsequent SmartZone creations will not invoke this splash screen.

3. The NetworkView dialog box will be displayed.

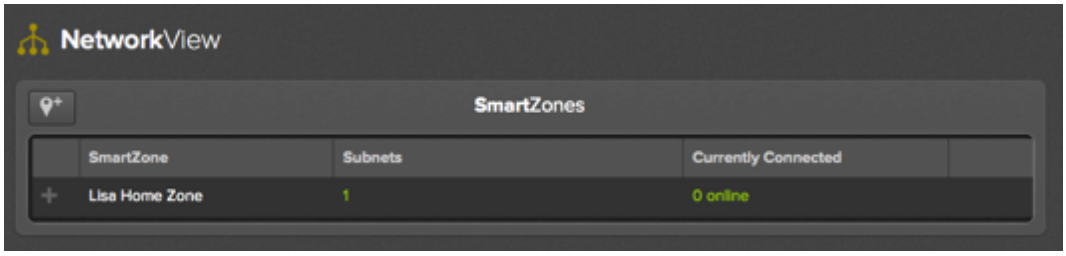


Figure 13. Adding a SmartZone.

4. To create a new SmartZone, click on the "Add Zone" icon in the upper left-hand corner of the dialog box.

5. The "Create SmartZone" dialog box displays. Here, you will select devices to add to your SmartZone and name the SmartZone.

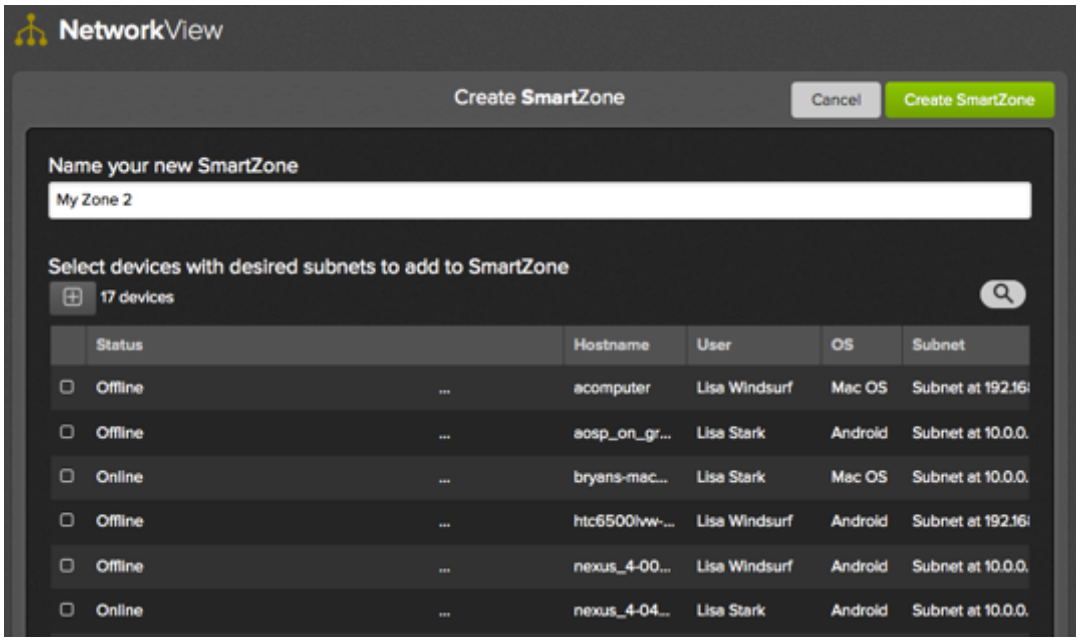


Figure 14. Selecting devices to add to a SmartZone.

6. Select devices to add to your SmartZone by clicking in the selection check-box at the far left of each device listed.
    a. Devices are shown in the list based on their membership by subnet.
    b. You may select one or more devices to add to a SmartZone.
7. Once you select one or more devices, add them to your SmartZone by clicking the "Add to the subnets list" icon immediately above the list of devices.
8. Name your SmartZone.
9. Click "Create SmartZone".
    a. The SmartZone is now created and devices within the SmartZone will use local traffic patterns and optimal name resolution for local network access.

Editing SmartZones

Once you create a SmartZone, similar patterns are used to edit an existing SmartZone.

NOTE: The "delete" icon (a trashcan symbol) and the "edit" icon (a pen/pencil symbol) to the far right of a list of SmartZones display when you hover over a specific SmartZone name.

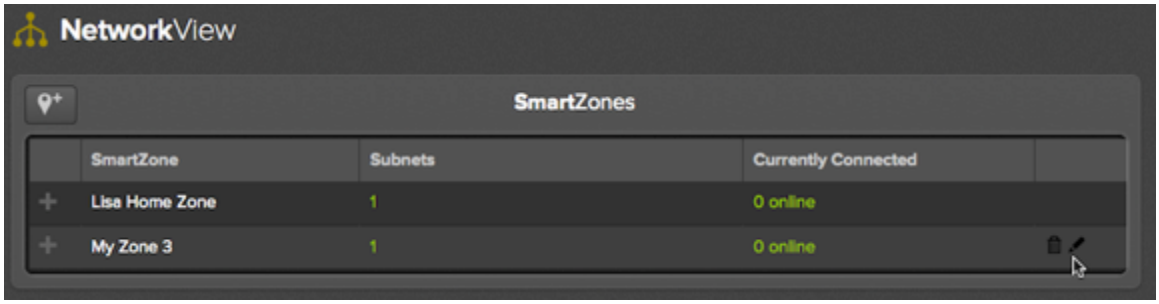


Figure 15. SmartZone editing icons.

1. Select the "edit" icon to edit the SmartZone name or device membership.
    a. The "Edit SmartZone" dialog box is displayed.

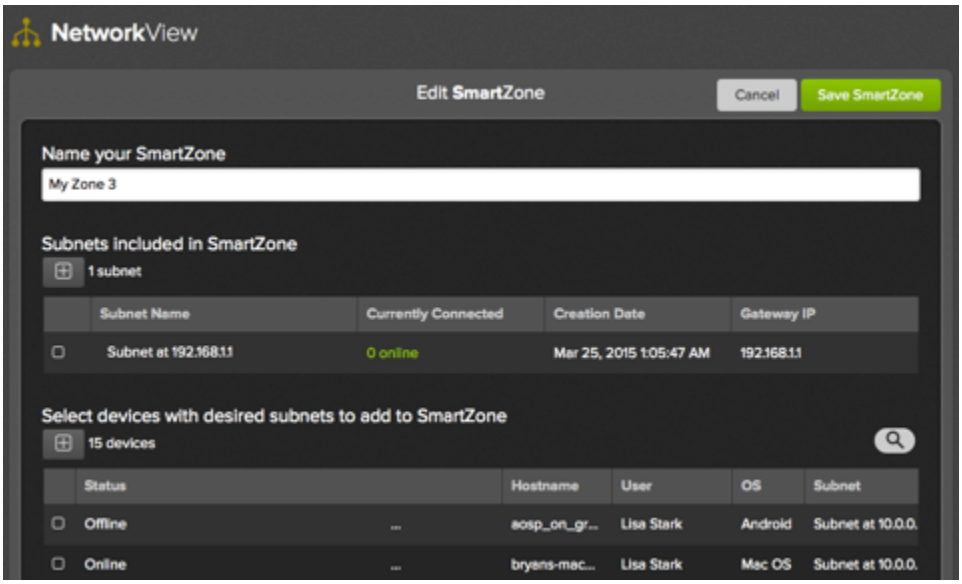


Figure 16. Editing a SmartZone.

2. Select the "delete" icon to delete the SmartZone.
    a. The "Delete" dialog box is displayed.

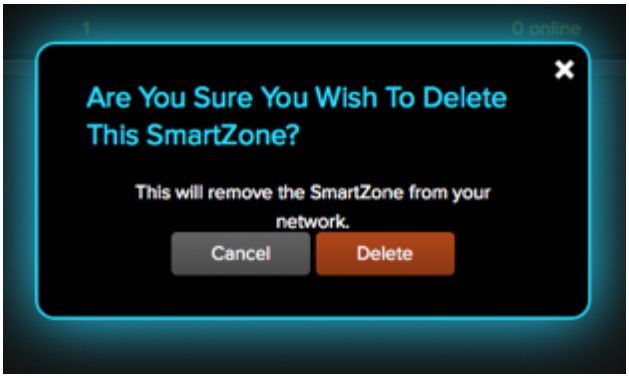


Figure 17. Deleting a SmartZone.

SmartZones with ADConnect

If you are using Pertino's ADConnect app, DNS responses from ADConnect-enabled DNS servers are filtered so that only non-Pertino addresses are received when two devices are in the same SmartZone. Likewise, if they are in different zones, only the Pertino addresses are received.

SmartZones with NameStation

NameStation is not affected by SmartZones.

MAC Address Implications

Any device that clones or duplicates MAC addresses for a router (either virtual or physical) could be problematic for a SmartZone. Traffic may not be directed to the proper resource.

Gateway

For systems and machines, such as printers and servers, that do not support the standard Pertino client, Pertino has developed the Gateway feature.

NOTE: The Pertino Gateway can be deployed locally or in AWS. For specific instructions on deploying in AWS, please consult support.pertino.com.

The Gateway enables deployments including:

- Customers who have specific policies that prohibit 3rd party clients to be installed on devices such as servers
- Products that do not support the Pertino client such as printers, security cameras, or time-card machines
- Remote users located in remote physical networks needing access to IT devices (such as databases or applications)
- Local users on the same or different subnets requiring access to similar devices where the Pertino client cannot be installed

NOTE: The Pertino Gateway can be enabled on Linux clients only. The following are the supported system requirements:

Linux Ubuntu Server 12.04	64-bit
4 cores	4 GB RAM

WARNING: To enable Gateway, Pertino modifies entries in the /proc/sys/net/ file system. These changes remain in place but will not persist across a reboot. Administrators should be aware that these modifications may occur at any time when a Pertino client has been installed. Please consult Pertino's Support site for more information.

Configuring your Router

You will need to add a route to your router configuration to enable communication between your network and the Gateway. This usually involves command-line or web access to a router's configuration. A typical CLI command might look like this:

```
$ ip route 50.203.224.0 /24 10.10.130.10
```

where 10.10.130.10 is the IPv4 address of the Pertino Gateway. This static route will need to be added to the site router configuration or to an Amazon VPC route table to enable connectivity to the Pertino Gateway.

Configuring Gateways

Enterprise-level customers can access the Gateway feature from the NetworkView app. Click on the "Gateways" toggle at the top of the page:

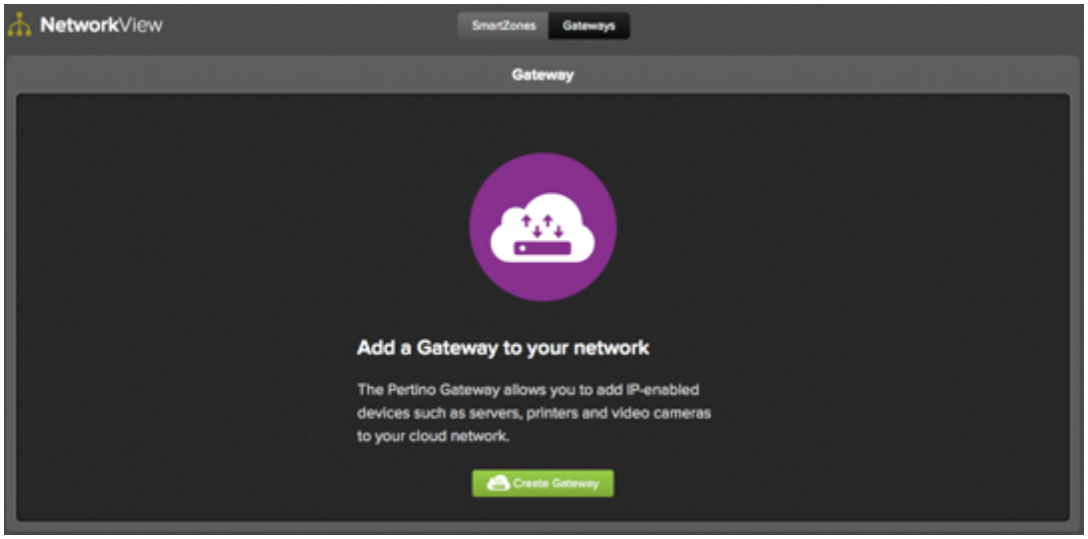


Figure 18. Gateway initial splash screen.

Creating a Gateway

1. Click the green "Create Gateway" button on the "Add a Gateway" screen.
    a. A screen with all available Linux clients will display.

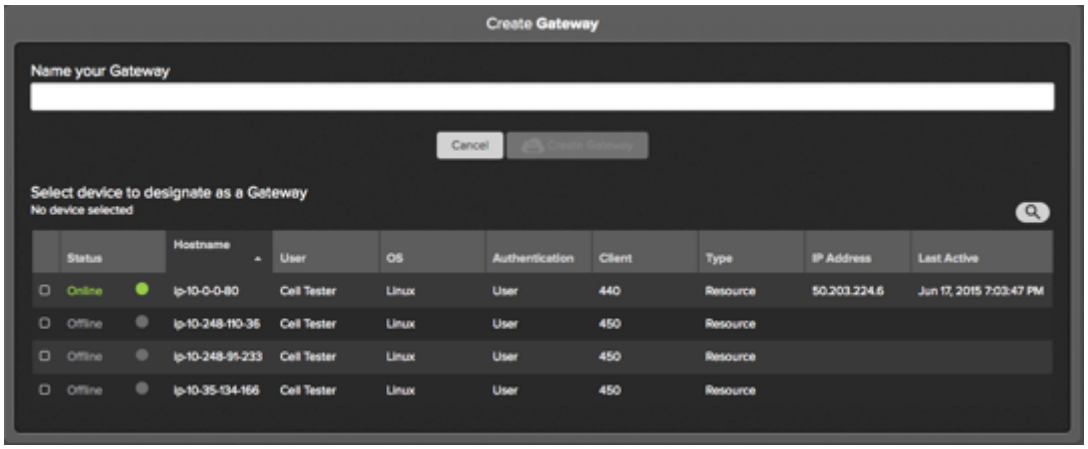


Figure 19. Naming your Gateway.

2. Enter a name for your Gateway in the "Name your Gateway" field.
    a. This is a "vanity" name that can be familiar to you.
3. Select a Linux client that you want to operate in Gateway mode in the "Select device to designate as a Gateway" panel immediately below.
    a. You may select only one, though you can create multiple Gateways in the overall process.
    b. The "Create Gateway" button will turn green when you have named a Gateway and selected a device.

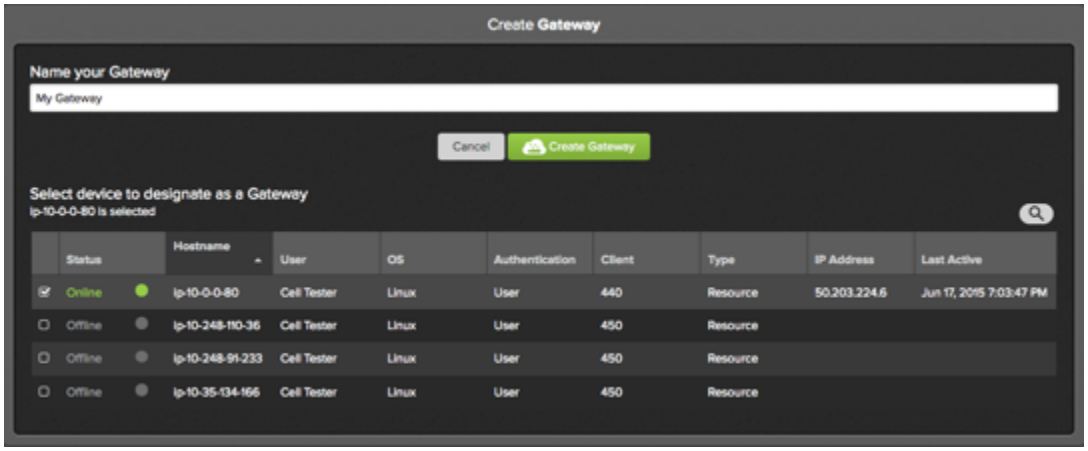


Figure 20. Designating a device as a Gateway.

4. Select "Create Gateway".
5. Your new Gateway will be displayed.

Figure 21. After adding a Gateway.

Adding devices to a Gateway

You must add devices to a specific Gateway to allow those devices to participate on a Pertino network.

1. Click the "plus" (+) sign next to your Gateway.
    a. The "Add devices" panel displays.

Figure 22. Adding devices to a Gateway.

2. You can add individual devices or import a list of devices in CSV format.

Adding Individual Devices

1. Click on the "plus" sign in the "Add devices" panel.
    a. Three input fields display – Hostname, Assign a custom name, and IP Address. These are required fields.
2. Enter the hostname of the device you want to associate to the Gateway.
    a. **WARNING**: Please limit the hostname to no more than 15 characters!
3. Enter the "Assign a custom name". This is a field for a custom description of the device.
4. Enter the IP address of the device you want to associate with the Gateway.
    a. **NOTE**: This IP address must be on the same subnet as the Gateway.
    b. You may enter add additional devices by clicking the "plus" sign multiple times.

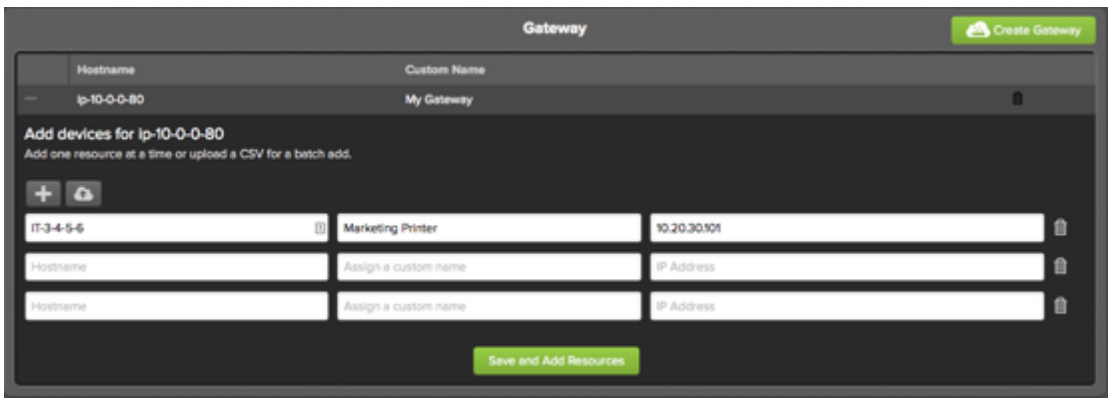


Figure 23. Adding multiple devices to a Gateway.

5. Click "Save and Add Resources".
    a. The Resource will be displayed in the panel immediately below.

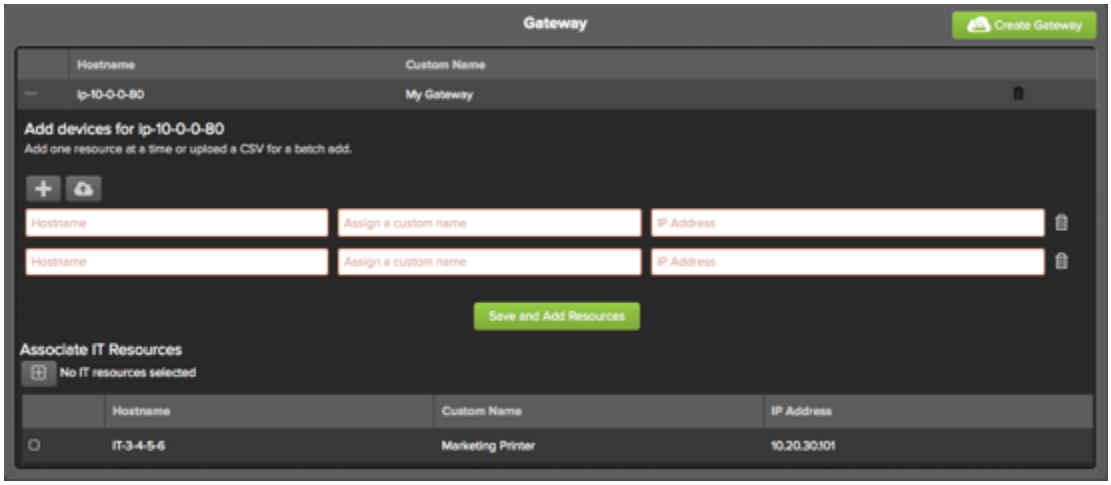


Figure 24. Saving devices to a Gateway.

Adding multiple devices in CSV format

You can add multiple devices in CSV format by clicking the "Upload" icon. A file browser will display requesting the CSV-formatted file to upload.

NOTE: Device fields in CSV format **MUST** be in the following order:

1. Hostname
2. Resource name
3. IP Address

WARNING: Please use Chrome or Safari to upload multiple devices in CSV format.

Confirming devices have been added

You can confirm devices have been added to the Gateway by navigating to the Device View screen and selecting the device you have associated to the Gateway.

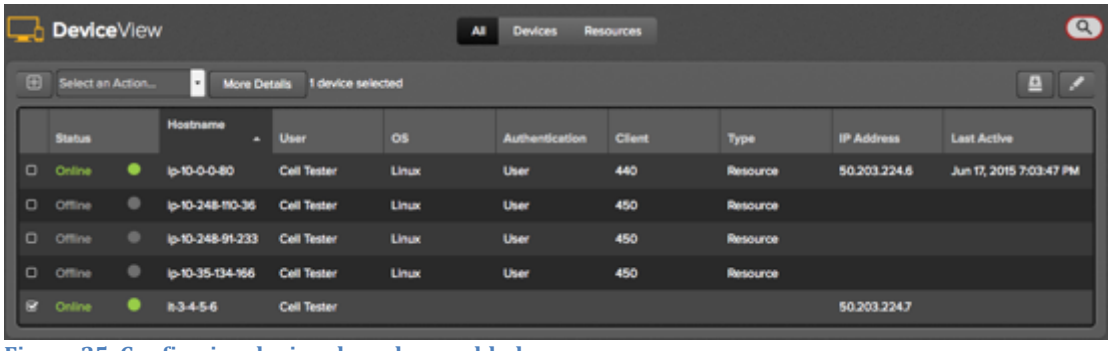


Figure 25. Confirming devices have been added.

By clicking on "More Details", you will notice that the device you have selected has been given a Pertino IP address:

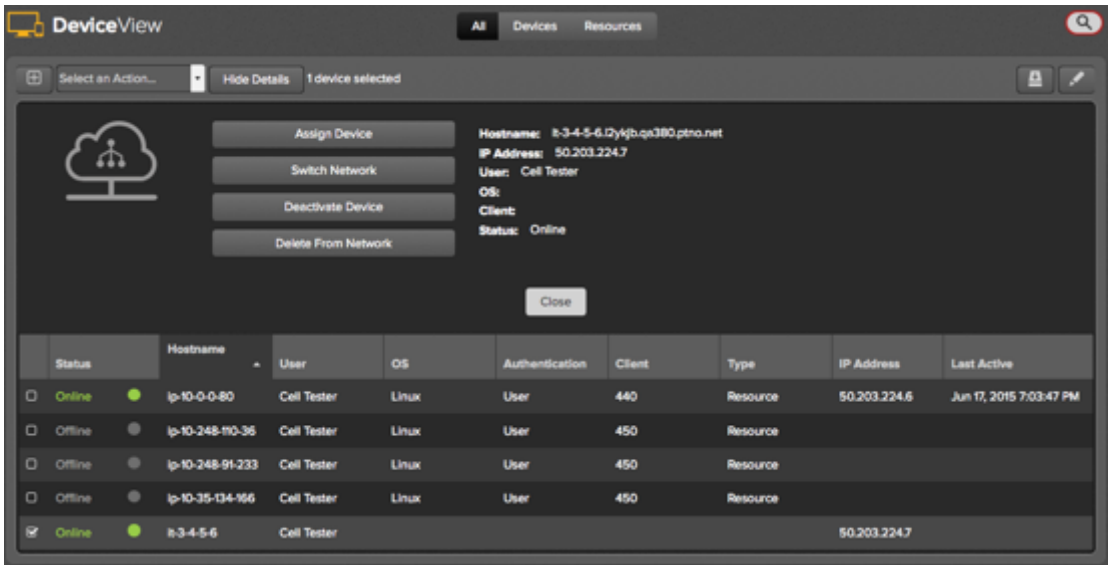


Figure 26. DeviceView showing devices added to a Pertino network.

NOTE: Fields such as OS, Authentication, Client, and Type will remain empty, as Pertino is unable to query the device for that information.

Converting a Gateway back to a Pertino client

You stop a Gateway from operating as a Gateway by converting that device back to a standard Pertino client.

1. Hover your mouse over the Gateway you wish to delete.
2. Click the "trash" icon that appears on the far right of that device.
3. A dialog box appears to confirm the deletion.
4. Click "Delete".

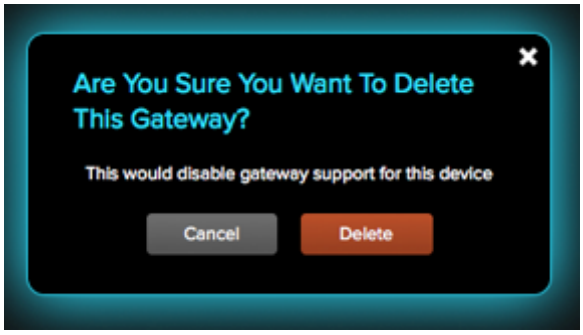


Figure 27. Deleting a Gateway.

NOTE: Deleting a Gateway does not remove it from the network. It converts the Gateway to a standard Pertino client.

Removing devices from a Gateway

You stop devices from communicating through a Gateway by using the "trash" icon.

1. From the "Associate IT Resources" panel, click the "trash" icon at the right for the device you no longer want to communicate through a Gateway.

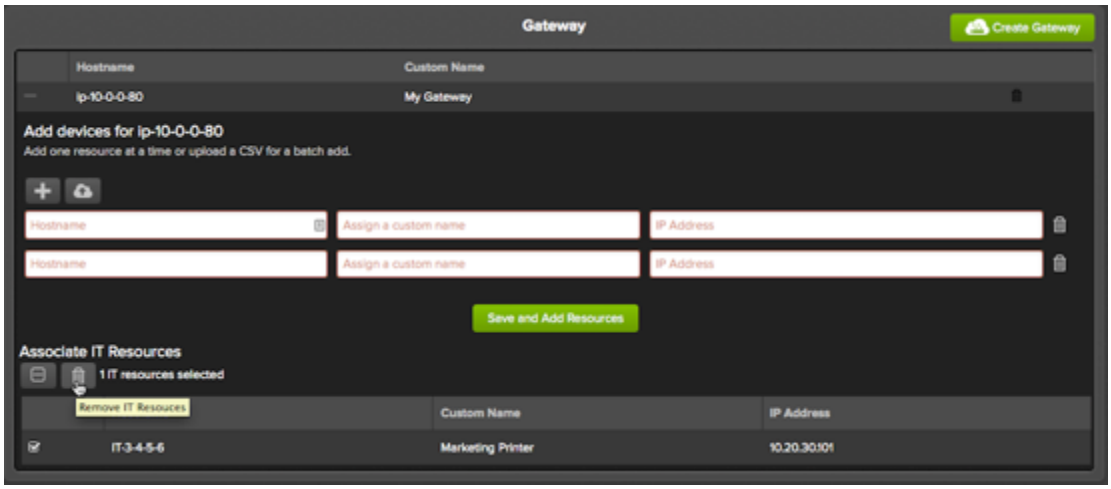


Figure 28. Removing devices.

2. A dialog box appears to confirm the deletion.
3. Click "Delete".

GeoView Pro

GeoView Pro tracks and maps the location of users and devices with street-level accuracy. Lost and stolen devices can be located and removed from the network with just a few clicks.

To enable GeoView Pro, visit the AppScape store and enable the App. Then navigate through MyApps to launch the app in the same manner as enabling NameStation.

The GeoView pro app displays all devices on your network on a world map. You can click on an individual pin icon to see details about that device.

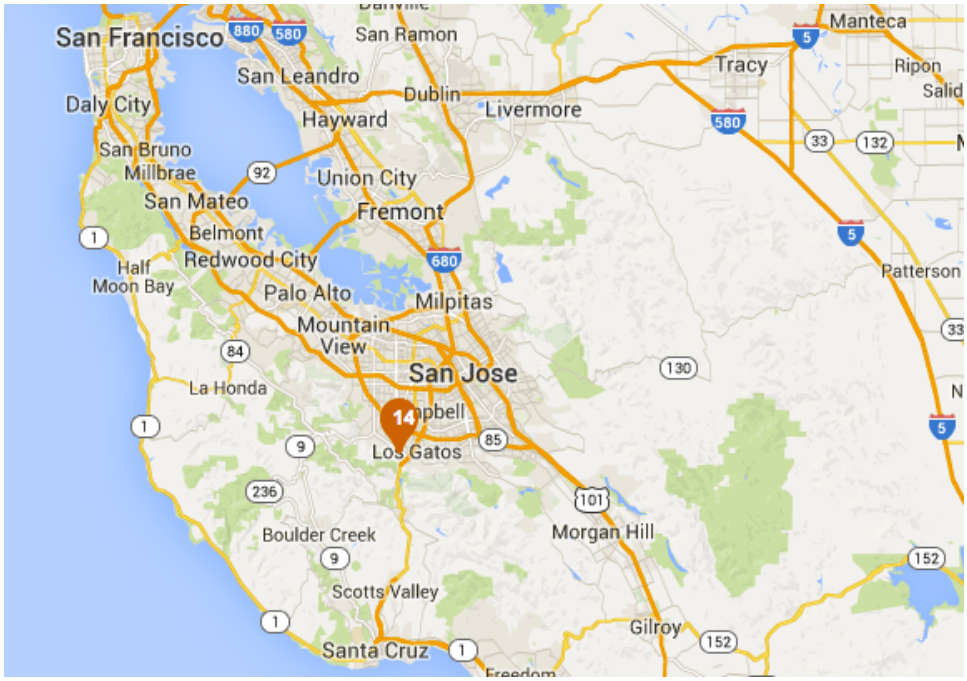


Figure 29. GeoView Pro showing high-level device location.

When multiple devices are in the same location, a numbered pin will be displayed showing how many there are. Clicking on the numbered pin will zoom in on the map to show just those devices.

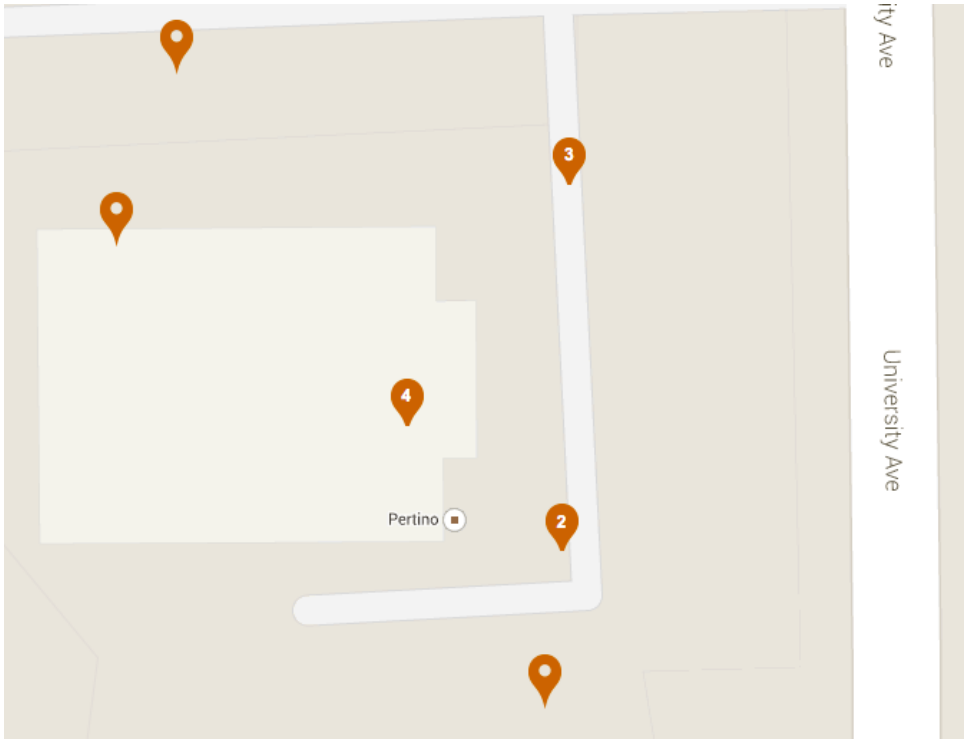


Figure 30. GeoView Pro zoomed in to show street-level view.

UsageMonitor

The UsageMonitor app lets you see how much data is flowing across your entire Pertino network. You can view the whole network at once, or drill down into individual members or devices.

Figure 31. Usage Monitor.

Top Users

The Top Users section shows the top 5 users and the amount of data they have transferred. Click on a user to drill down and get detailed information about their data usage and which devices they are using.

Top Devices

Like Top Users, the Top Devices section shows the top 5 devices and the amount of data they have transferred across the Pertino network. Click on a device to drill down.

Total Usage chart

The main chart shows the total volume of traffic across the entire network. Click on a point in the chart to display the top devices at that time on the right-hand side. If you see a spike in data usage in the main chart, you can click on the peak to see what device or devices were most active during the spike.

Time periods and data values

UsageMonitor has a toggle between 1 day and 7 day views at the top of every screen.

- In the 1-day view, data is displayed in 5-minute increments for the previous 24 hours

- In the 7-day view, data is displayed in 1-hour increments for the previous week.
- Traffic volume is measured in both directions (upload and download)
- A file server accessed by many users will show a large volume of upload traffic. The data is uploaded from the server, travels across the cloud and appears as download volume at the end user's device.
- Aggregate views will show equal amounts of upload and download volume.
- When a user accesses a file, the traffic is uploaded from the server and downloaded by the client. When the "whole network" is viewed, data from both sides of the transaction is included.

  NOTE: Most end user devices will show more download volume than upload.

Dashboard

When UsageMonitor is enabled, a graph is added to the main Dashboard in the web management console to display a week's worth of bandwidth usage on your network. Clicking on the Dashboard graph takes you straight to the UsageMonitor app. See Figure 4.

SecurityPolicy

The Security Policy App enables you to create security rules within a network, restricting access between devices and servers within that network. These rules are similar to network “ACLs”, where access is allowed or denied between a source device and a destination device using device hostnames and a port/protocol definition. The SecurityPolicy App is available with Enterprise plans.

Activating SecurityPolicy

As with the other Apps within AppScape, you'll need to activate SecurityPolicy. When you click the "Activate" button, a brief overview immediately below the app is displayed.

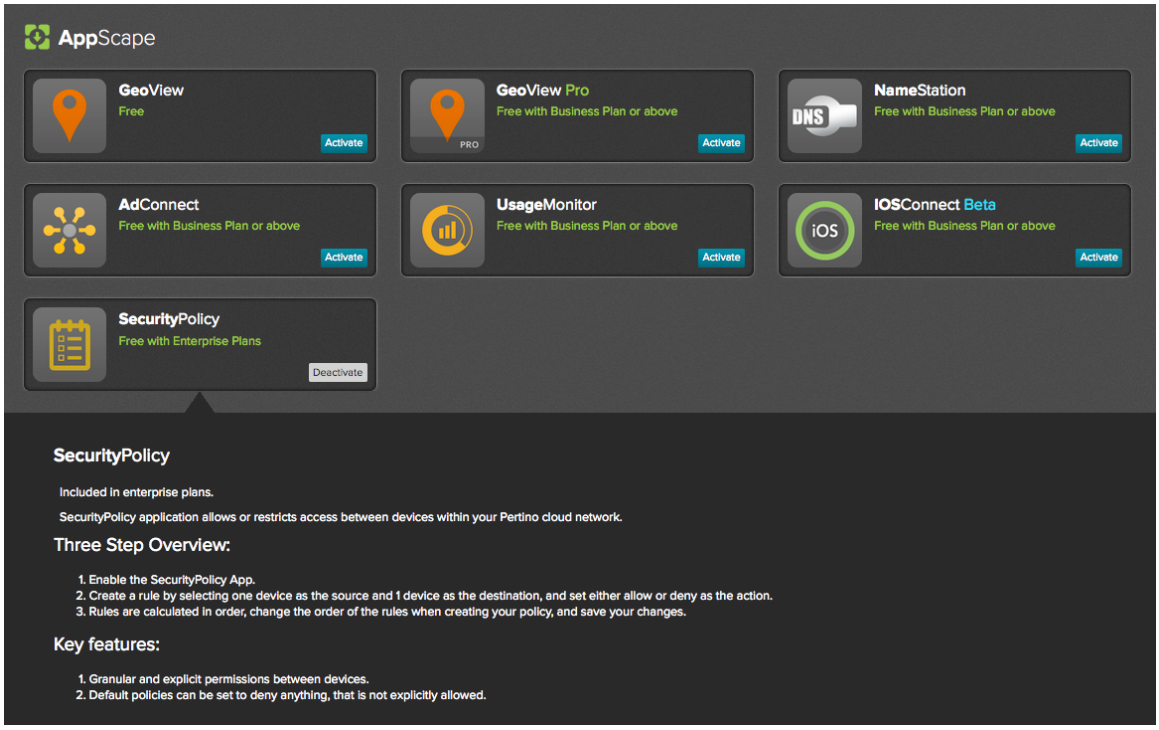


Figure 32. Activate SecurityPolicy app.

After activating the SecurityPolicy app, you can begin using it from the MyApps pane.

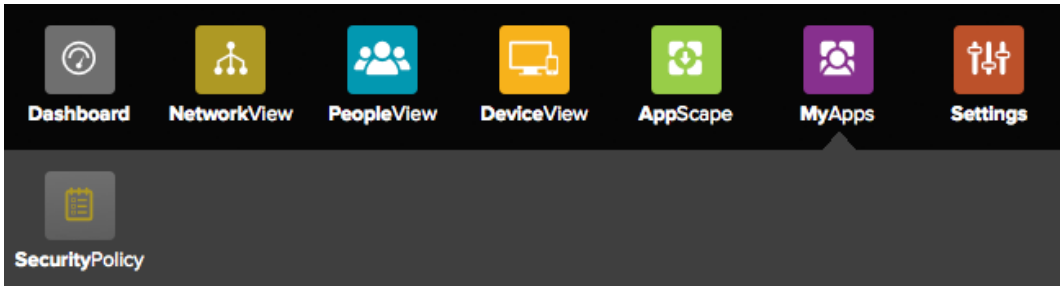


Figure 33. SecurityPolicy in the MyApps pane.

IMPORTANT: By default, all networks have an ("ANY" "ANY" "ANY" "Allow") rule defined, meaning that any device can talk to any other devices, on any port/protocol.

Creating a new policy rule

1. In the Rule pane, click on the "Create Rule" button.

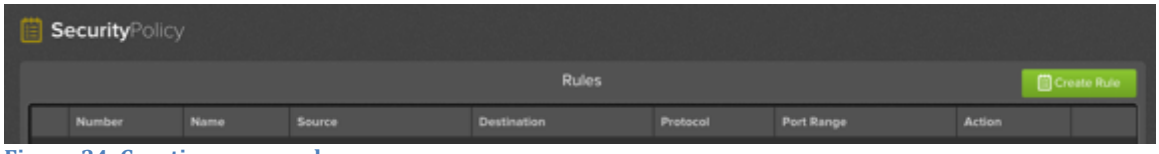


Figure 34. Creating a new rule.

2. This will add a new row, where you can specify what you want to allow or deny.

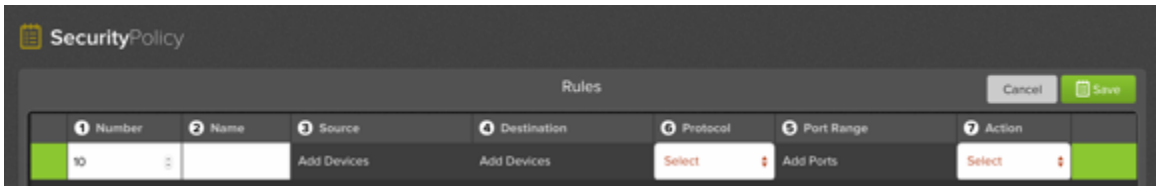


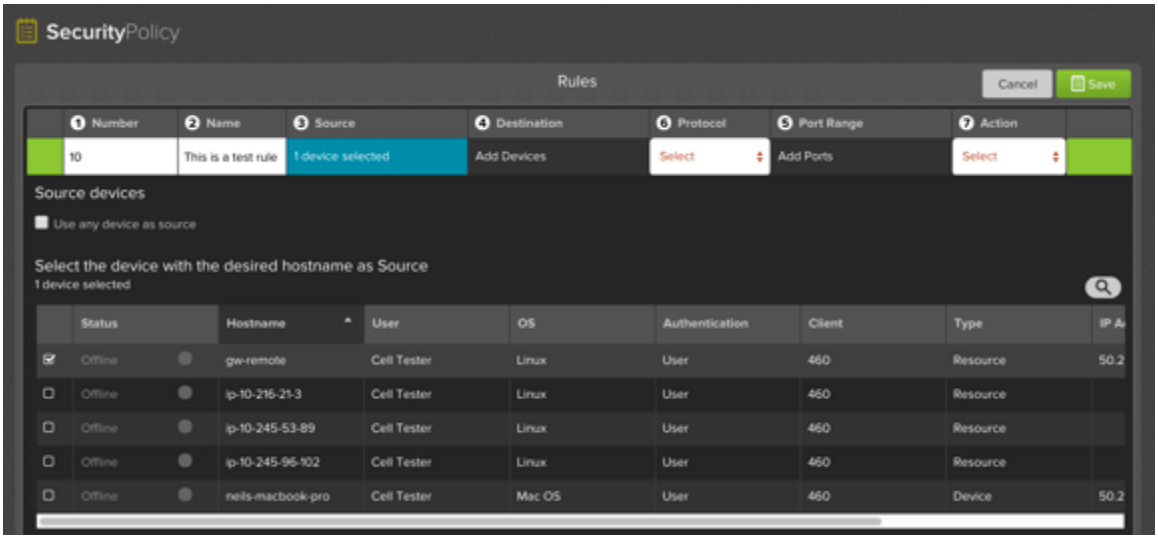
Figure 35. Specifying allow or deny in a new rule.

3. Next, define the rule number.

   NOTE: All rules are analyzed in order, e.g. rule 1, then rule 2, then rule 3, etc. For example, if your first rule is to allow access to "ANY" device and your second rule is to deny access to a device, the second rule will not be "hit". *Changing the order of the rules will ensure the correct policy is applied.*

   NOTE: Rules will reorder automatically. For example if we create a new rule and give it position number #10. If there is an existing rule at position 10, that rule will become #11 and the new rule will be # 10. All other rules below that number will reorder, i.e. 11, 12, 13, 14, 15, etc.

4. Add a rule name. The rule name helps add a description so that you and other admins can quickly understand what the rule intends to do.

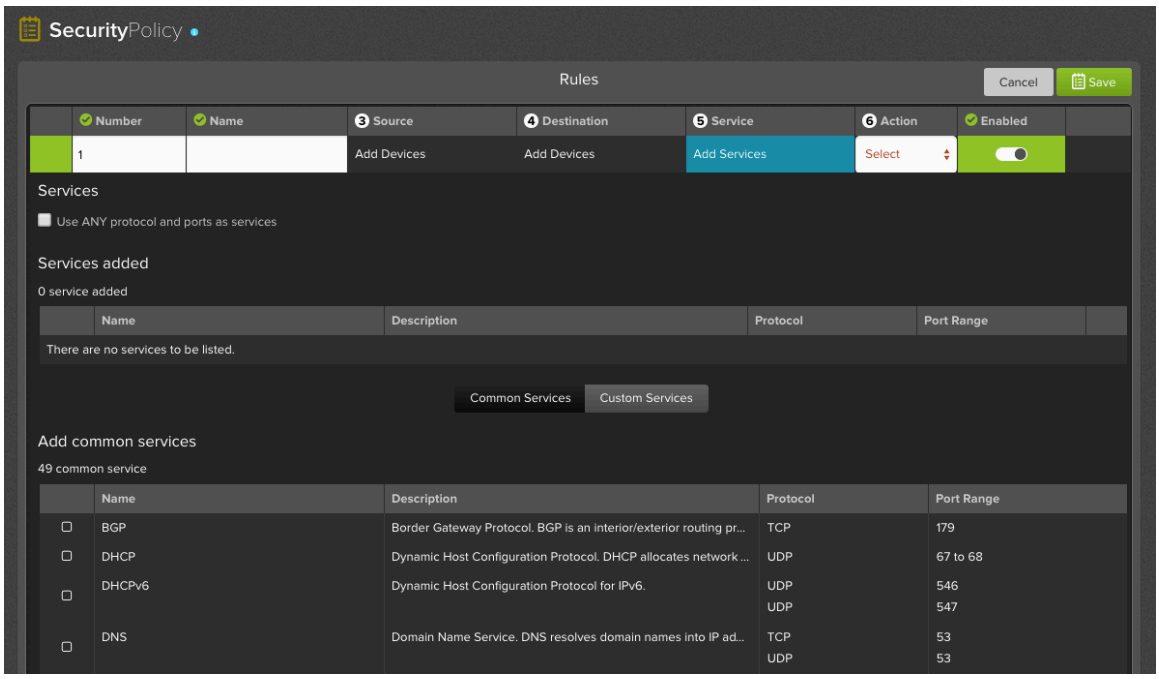


5. Then, identify the source device, or from which device will traffic be allowed.
   a. A single device, multiple devices or a user can be selected, or "ANY" device can be selected with the checkbox above.

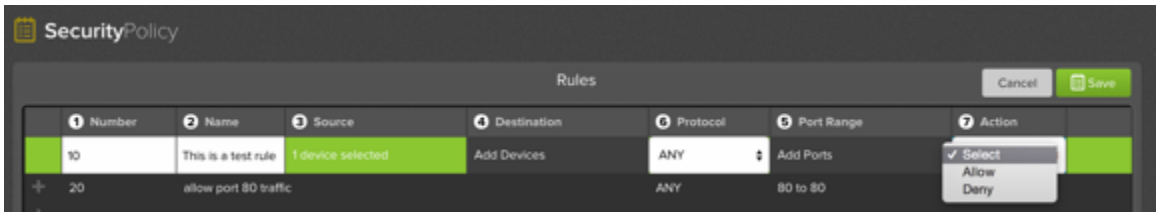
NOTE: When selecting a user, all devices that has authenticated with that username and password will be included with this security rule. This also applies for new devices. For example, Joe downloads and logs into the Pertino client on a new device with his credentials, that device will automatically be included into any security policy that allows or denies Joe access.

6. Next, specify the destination device to where traffic will be allowed. This step is identical to Step 5, immediately above.

7. Next, specify the Service. The admin can specify one or mode of the common and predefined services, for example (FTP, HTTP, SSH, etc). Alternatively the admin can define a custom service be specifying the protocol and the port number.



8. Then, specify whether this is an "allow" rule or a "deny" rule.



9. Finally, Save the rule to commit the change.
    a. You will receive an error if any of the fields are missing or have incorrect data.

NOTE: You can edit the rule number or any other field with the edit (pencil) icon. Additionally you can also delete the rule with the delete (trash) icon.

After you continue to add security rules and have finalized your security policy. You can change the default allow rule to a deny rule, ensuring that only the traffic you have specified will be permitted.

NOTE: The default rule cannot be deleted. Its order cannot be changed—it will *always* be the last rule in the policy list.

Advanced Deployment Information

Pertino offers numerous options to customize your deployment. The following section provides some information on each option.

DNS

Name resolution is a critical aspect of any network and it's no different with Pertino. When one computer needs to connect with another, the first step is to resolve the destination computer's name to an IP address. There are several different ways to resolve names and each has it's own interaction with Pertino networks.

Pertino Fully Qualified Domain Names

As mentioned in the NameStation section of this document, Pertino automatically assigns a name to every computer on the network. These take the form of **hostname.subdomain.pertino.net**.

These names will ALWAYS resolve to Pertino IP addresses. When two computers are on the same local network, using these names will cause traffic between them to be routed through the Pertino cloud.

External Fully Qualified Domain Names

If you have published DNS records for any servers, like www.mycompany.com, these will continue to resolve to the IP addresses you specify. These will not resolve to Pertino IP addresses unless you specify one. Some network administrators will use CNAME records to point their own names to Pertino resources. For example, **intranet.mycompany.com** can point to the Pertino host at **server4.mycompany.pertino.net**.

Local Resolution

Various client computers use several local name resolution protocols.

- Windows primarily uses LLMNR (Link-Local Multicast Name Resolution)
- Mac OS X primarily uses mDNS (multicast Domain Name System)

Network behavior differs depending on the location of devices. For example:

1. When two computers are on the same local network, local name resolution will result in computers finding each other locally.
    a. Even if they are both part of the Pertino network, traffic between them will stay on the local network.
2. When two computers are on the Pertino network but not local to each other (for example, one in the office and one on a home network)
    a. Pertino will enhance the local name resolution protocols so that these machines can find each other, even though they are not local to each other.
    b. Traffic between these two computers will flow across the Pertino network.

Active Directory Name Resolution

Active Directory name resolution can be complex. The following list provides some guidance on how AD works in a Pertino environment.

1. All member computers (both clients and servers) will announce their IP addresses to the AD DNS servers.
2. Computers connected to a Pertino network are multi-homed—they have both a local and a Pertino IP address.

    NOTE: *Both* addresses are submitted to the AD DNS servers.

3. When an AD DNS server running Pertino is asked to resolve a name for a server that is not on the Pertino network:
    a. There is no Pertino IP address, so the local IP address is returned.

4. If the client is on the Pertino network and does not have local connectivity to the server, the connection will fail.
5. If the client is on the Pertino network but also has local connectivity to the server, the connection will succeed.
6. When an AD DNS server running Pertino is asked to resolve a name for a server that is also on the Pertino network:
    a. There is both a Pertino IP and a local IP in the DNS server's database.
7. If the client is on the Pertino network and does not have local connectivity to the server, the Pertino IP will be returned and the connection will succeed over the Pertino network.
8. If the client is on the Pertino network and also has local connectivity to the server, the local IP will be returned and the connection will succeed across the local network.
9. If the client is NOT on the Pertino network, the local IP will be returned and the connection will succeed across the local network.

    NOTE: AD DNS servers NOT running Pertino are NOT supported.

10. To use ADConnect, you must have Pertino installed on every domain member server running the DNS role. See the **Error! Reference source not found.** section above.
11. If an AD DNS server NOT running Pertino is asked to resolve a name for a server that is on the Pertino network
    a. The client is—by definition—also not on the Pertino network
    b. Otherwise, it could not connect to the AD DNS server
    c. Both the local and the Pertino IP addresses will be returned to the client and there is no deterministic way to know which IP address it will use.
    d. The result would be clients that can connect to that server sometimes, but not always.

System Requirements

The latest supported devices and device versions can be found at:
https://support.pertino.com/hc/en-us/articles/200488469-System-Requirements

Linux servers

Pertino officially supports Ubuntu, RedHat, and CentOS servers. Debian and RPM packages are available for download and you are welcome to try installing on other distributions as well. If you're reading this section, you may have the technical background to begin the installation. The Linux download page, available at http://pertino.com/download-linux, has instructions for installing with apt, dpkg, and yum, as well as providing example Chef and Puppet scripts.

Linux servers are automatically marked as Resources when they join a Pertino network.

Mobile Devices

For many users, mobile devices are becoming the default way to access company data and services. Pertino offers connectivity from both Android and iOS devices.

Android

The Pertino Android app is available on Google Play. Pertino for Android enables mobile users to securely access files, desktops, and applications from anywhere. After a user logs in to the Pertino network, the Android app has three main sections.

1. From the People section, easily contact people in your Pertino network.
2. From the Devices section, connect to your remote desktops or servers using the integrated experience with Microsoft RDP client.

   NOTE: You can leverage the Pertino cloud network via other RDP clients as well, but you would need to configure a desktop connection within those apps. Our Support does not extend to issues encountered with other RDP clients.

3. From the Files section, connect to file shares on Windows and Macs connected to your Pertino network.
   a. We recommend ES File Explorer, but there are many file access apps on Google Play.

Switch networks easily using the Network icon in the navigation panel at the bottom.

iOS

iPads and iPhones have an IPSEC VPN client as part of the OS. Pertino leverages this built-in functionality to connect iOS devices to non-mobile devices on your Pertino cloud network. iOS connectivity is offered as a Beta through the iOSConnect Beta app in the AppScape store. Please see iOS Beta v2 FAQ for more information.

Support and Feedback

Please contact support@pertino.com with any issues you encounter and to provide feedback on your experience with the Pertino product.