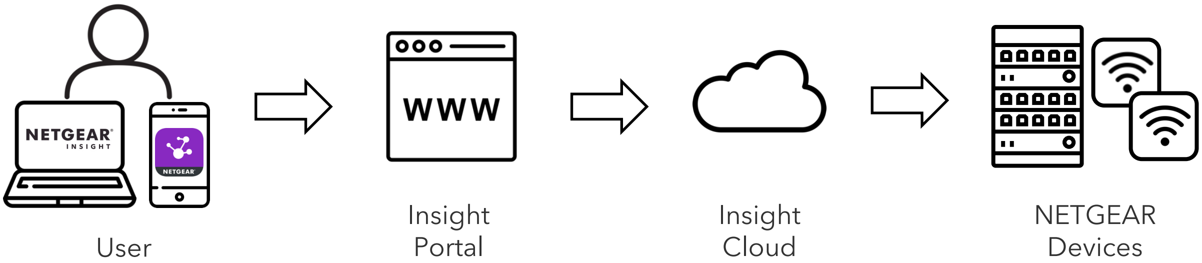
NETGEAR Insight Architecture

NETGEAR® Insight™ is a Cloud-based management platform that enables easy setup and configuration of NETGEAR® Total Network Solution devices, including Routers, Switches and Wireless Access Points. Insight offers control of multiple customer systems in multi-location, providing secure connectivity, scalability and reliability at an affordable price.

Insight Cloud

Insight is an industry-first approach to multi-site and multi-device network management for small and medium businesses.

The Insight software agent, which interfaces with the Insight app, is built into our Total Network Solution devices, creating an ecosystem of products that can be managed on a single pane of glass remotely, via web-browser or smartphone app.



The Insight Cloud is composed of several Insight Cloud servers operating in clusters behind load balancers. These servers are elastic and can be scaled up or down as per the demand. All servers back up data on a regular basis for business operation continuity assurance.

If the system loses connection with the Insight Cloud server, the Insight managed devices will still work and keep their functionality. However, on-line firmware updates and settings can not be pushed to devices remotely, and a few other limitations in the operations of the Insight managed devices.

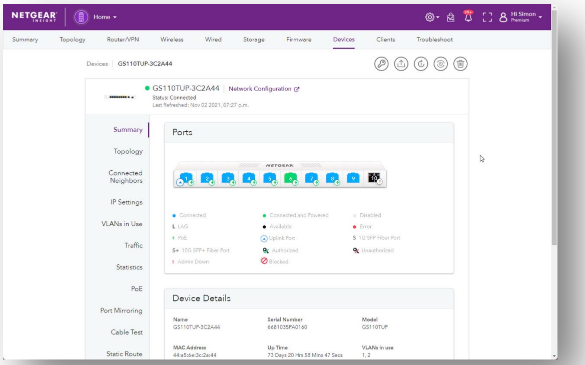
Insight Cloud Portal Values

- Simplifies network management of various types of devices including routers, switches, wireless access points.
- Saves significantly network admin's time and cost by reducing visits to sites.
- Allows system integrators and MSPs to use Insight as the only tool to monitor multiple customers in multiple locations through one dashboard.
- Notifies network engineers timely for any network problems through mobile app push notifications and emails.

Insight Web-Interface

The Insight Cloud Portal is the website that provides access to the Insight cloud-based management platform. With an intuitive dashboard, admins can have continuous visibility of the system and client health for each network location. It also provides access to detailed information about each device at a network location.

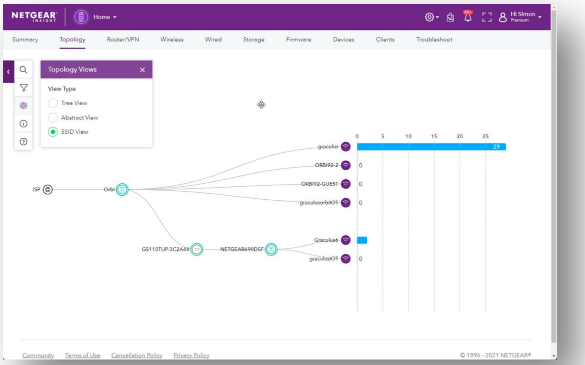
Users can customize the dashboard by adding or removing predefined widgets. In a widget, you can customize the information that displays in the widget.



GS110TUP-3C2A44
Status: Connected
Last Refreshed: Nov 02 2021, 07:27 p.m.

Device Details

Name	Serial Number	Model
GS110TUP-3C2A44	6681035PA0160	GS110TUP
MAC Address	**Up Time**	**VLANs in use**
44:a5:6e:3c:2a:44	73 Days 20 Hrs 58 Mins 47 Secs	1, 2

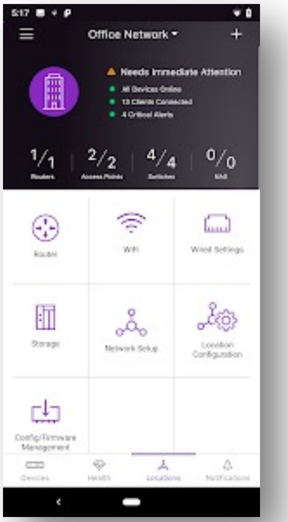


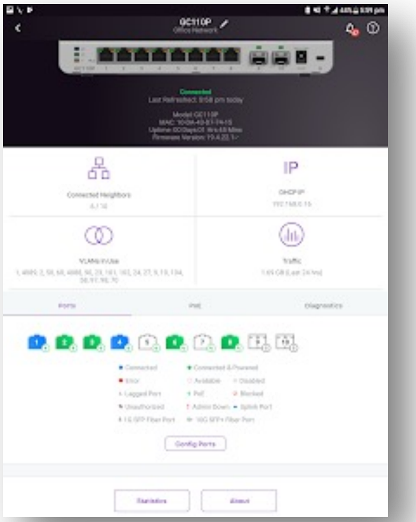
Screenshots of the web-browser interface

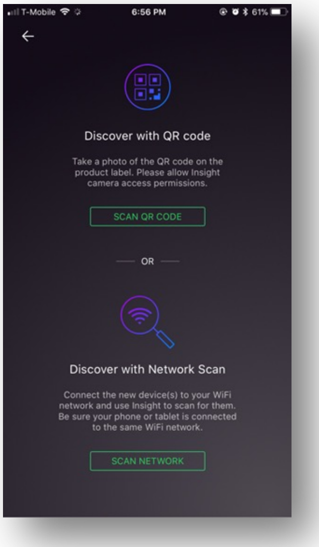
Insight App

The Insight mobile app is the application for Android and iOS smartphones.

Insight app will have a subset of features supported by the browser. Not all configurations are exposed on Mobile GUI







Discover with QR code

Take a photo of the QR code on the product label. Please allow Insight camera access permissions.

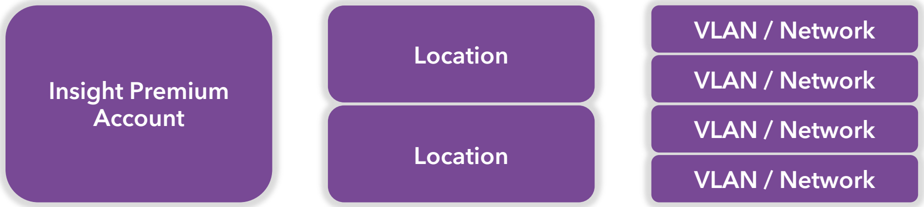
Discover with Network Scan

Connect the new device(s) to your WiFi network and use Insight to scan for them. Be sure your phone or tablet is connected to the same WiFi network.

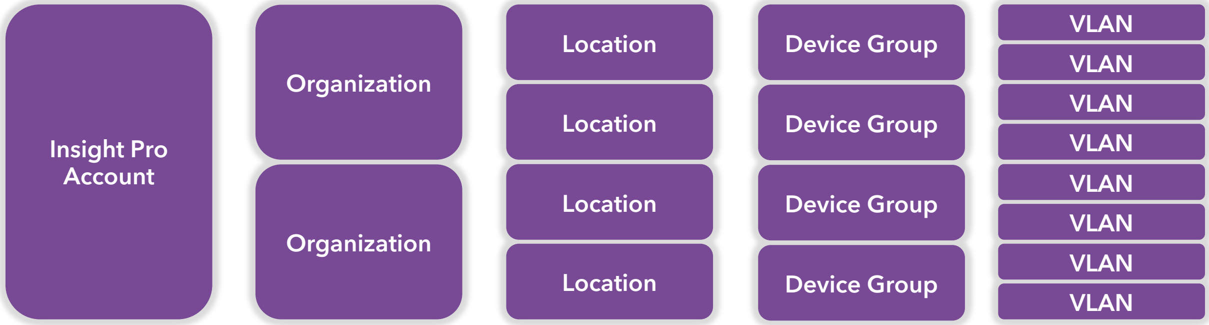
Screenshots of the smartphone app

Designed to fit businesses of all sizes, NETGEAR Insight is available in 2 subscription plans, Premium and Pro.

NETGEAR Insight Premium is ideal to support single businesses that can have multiple locations and remote workforce networks.



Upgrade to **NETGEAR Insight Pro** to manage multiple customers and add new features, and hierarchical levels.



Account holder: The individual or business that initiates and owns the Insight subscription and the NETGEAR managed devices in the network.

Organization: A company or customer that is served by Insight management. Only available for Insight Pro accounts.

Location: A subaccount of an Insight organization and refers to the physical site where the devices reside. An Insight account can support multiple network locations.

Device Group: is a level of hierarchy below an Insight Location where a group of devices can be added with certain common configurations.

VLAN / Network: A logical container for a set of centrally managed devices and services.

Data Storage

All customer management data is replicated across independent same-region data storage in real time. The same data is also replicated in automatic daily archival backups hosted by in-region cloud storage services:

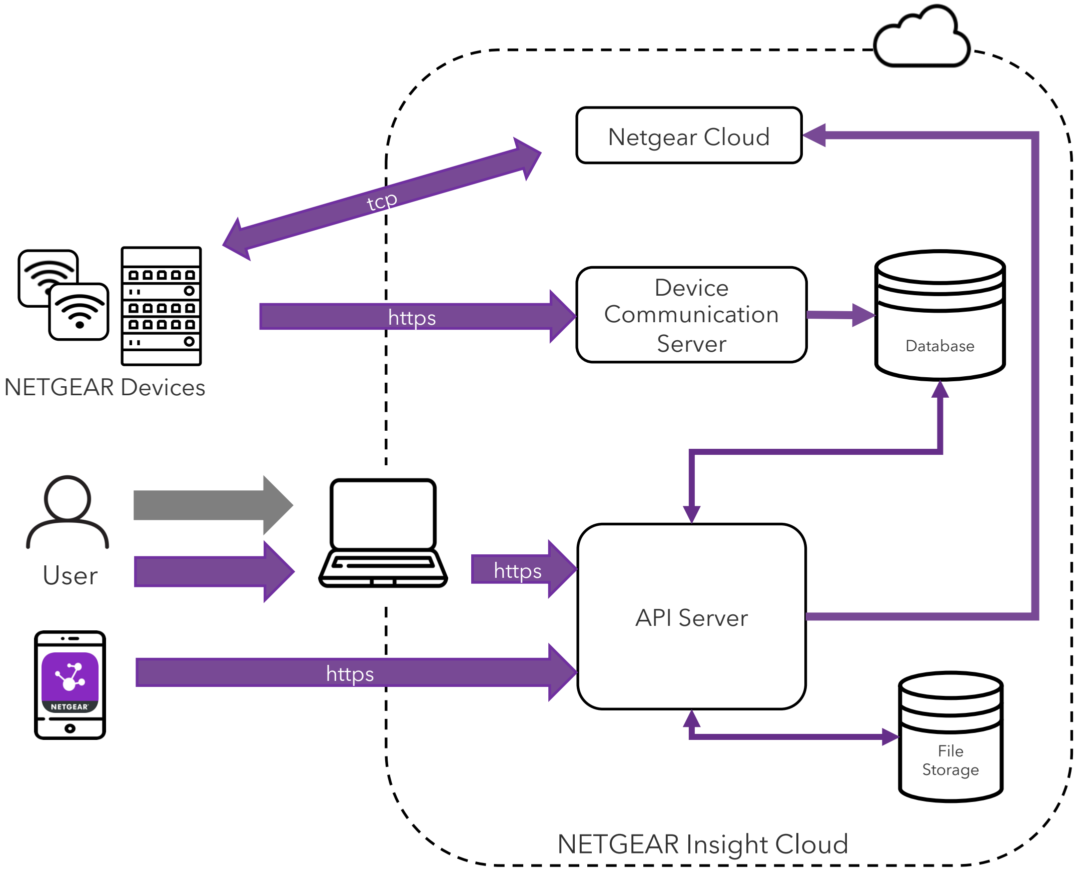
- USA - Oregon
- Europe – Ireland

NOTE: NETGEAR does not sell any of these data.
End customer traffic does not come to the Insight cloud.
For T&C please refer to https://www.netgear.com/about/terms-and-conditions/

NETGEAR® One Cloud Infrastructure

With decades of experience selling cloud-managed and cloud-accessible storage solutions, NETGEAR® has the infrastructure to support TNS these applications. What we refer to as NETGEAR One Cloud, is the foundation for Insight Cloud.

Insight High Level Architecture



➡ **Management data:** The data (configuration, statistics, monitoring, etc.) that flows from NETGEAR devices to the cloud over a secure internet connection.

➡ **Private data:** Data related to user traffic (web browsing, internal apps, etc.) does not flow through the NETGEAR® One Cloud. It goes directly to their destination on the LAN or across the WAN.

Service Level Agreement

NETGEAR® has 365 days, 24/7 DevOps teams that ensure cloud operations and security.

On our status.netgear.com page, users can check in on our One Cloud services

Bookmark the Insight Cloud Status link status.netgear.com/insight

Firewall Troubleshooting

If your firewall restricts access to certain domains or ports, your Insight devices might not be able to reach Insight cloud services. Insight Managed devices cannot be configured or monitored with Insight if they cannot reach Insight cloud services.

Make sure that the following domains and ports are not in your firewall's blocklist. If your firewall uses an allow list, add the following domains and ports to your firewall's allow list.

	Domains	Port
1	registration.ngxcld.com	443
2	advisor.ngxcld.com	443
3	presence.ngxcld.com	443
4	devcom.insight.netgear.com	443
5	api.insight.netgear.com	443
6	presence.insight.netgear.com	443
7	xbroker-z1-i21.ngxcld.com; xbroker-z1-i22.ngxcld.com xbroker-z1-i23.ngxcld.com; xbroker-z1-i24.ngxcld.com xbroker-z1-i25.ngxcld.com; xbroker-z1-i1.ngxcld.com xbroker-z1-i2.ngxcld.com; xbroker-z1-i3.ngxcld.com xbroker-z1-i4.ngxcld.com; xbroker-z1-i5.ngxcld.com xbroker-z1-i6.ngxcld.com; xbroker-z1-i7.ngxcld.com xbroker-z1-i8.ngxcld.com; xbroker-z1-i9.ngxcld.com xbroker-z1-i10.ngxcld.com; xbroker-z2-i1.ngxcld.com xbroker-z2-i2.ngxcld.com; xbroker-z2-i3.ngxcld.com xbroker-z2-i4.ngxcld.com; xbroker-z2-i5.ngxcld.com xbroker-z2-i6.ngxcld.com; xbroker-z2-i7.ngxcld.com xbroker-z2-i8.ngxcld.com; xbroker-z2-i9.ngxcld.com xbroker-z2-i10.ngxcld.com; xbroker-z2-i11.ngxcld.com xbroker-z2-i12.ngxcld.com; xbroker-z2-i13.ngxcld.com xbroker-z2-i14.ngxcld.com; xbroker-z2-i15.ngxcld.com xbroker-z2-i16.ngxcld.com; xbroker-z2-i17.ngxcld.com xbroker-z2-i18.ngxcld.com; xbroker-z2-i19.ngxcld.com xbroker-z2-i20.ngxcld.com; xbroker-z2-i21.ngxcld.com xbroker-z2-i22.ngxcld.com; xbroker-z2-i23.ngxcld.com xbroker-z2-i24.ngxcld.com	443
8	monitor.insight.netgear.com	443
9	insight-firmware-prod.s3.amazonaws.com	443

Check the link for additional port exceptions: https://kb.netgear.com/000062467

GDPR and Privacy

NETGEAR® recognizes the worldwide importance of privacy, security, and data protection to our customers, partners, and employees.

Our Cybersecurity Committee is tasked with the oversight and monitoring of NETGEAR's privacy and data security and regularly engages with outside experts regarding various privacy issues including privacy by design and encryption.

For more information visit: https://kb.netgear.com/000058808/GDPR-and-Privacy

FAQ

How does Insight compare to other cloud management solutions?

Insight is designed to be more secure than solutions that require firewall exceptions, opened ports, separate servers, proxies, or special configuration. Insight does not require these kinds of exceptions because the Insight devices themselves are responsible for all communication outside of the subnet. These protections makes it far less likely that an external entity would be able to initiate this dialogue or to compromise the Insight communication model without gaining physical access to your network.

How does the NETGEAR One Cloud server deter break-ins?

NETGEAR One Cloud servers have strong password protection and are accessible only through Secure Shell (SSH) protocol on a private IP address. On the One Cloud servers' public interface, only HTTPS secure access is enabled with the certificate authority-signed Secure Sockets Layer (SSL) certificate. Users can only access their own information after being authenticated with their email address and password. Insight has strict password rules, 2FA (Two Factor Authentication) support and users can't reset their password without email access.

How does NETGEAR keep communication between One Cloud servers and Insight devices secure?

Insight devices reject communication that is not validated as originating from the NETGEAR One Cloud servers. Users must log in with their Insight account password to see device information or change any settings. Without user authentication, Insight devices only send keep-alive messages to the NETGEAR One Cloud servers.

What protects an Insight device from being an attack vector into my network?

Before connecting with the NETGEAR One Cloud server, Insight devices are similar to other web-managed network devices. After an Insight device is associated with an Insight account, it is designed to reject all other attempts to communicate with it. Because you do not need to open any ports on existing firewalls, your network remains more secure. The Insight-enabled management mode greatly reduces the risk of the device being used as a remote proxy in an attack.

Will my firewall prevent Insight from working?

The connection from an Insight device to a One Cloud server is initiated from behind the firewall instead of being requested from outside the firewall. By default, firewalls do not prevent traffic generated behind the firewall from going out.

If your firewall is set to block, filter, or redirect certain outgoing traffic, this could inhibit contact between an Insight-managed device and NETGEAR's One Cloud service. Our beta testing and production monitoring have found no examples of such problems so far. The Insight cloud service works with most common firewall configurations. If your firewall setup is very strict, you must define a specific rule to allow outbound access to the Insight server.

©2023 NETGEAR®, Inc. NETGEAR®, the NETGEAR® logo, and Insight™ are trademarks and / or registered trademarks of NETGEAR®, Inc. and/or its subsidiaries in the United States and/or other countries.
Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. All rights reserved.