USER GUIDE

inseego

Inseego Secure

IoT Privacy and Cybersecurity Platform

INSEEGO COPYRIGHT STATEMENT

SOFTWARE LICENSE

Proprietary Rights Provisions:
Any software drivers provided with this product are copyrighted by Inseego Corp. and/or Inseego Corp.'s suppliers. Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp. and/or Inseego Corp. suppliers. The disassembly, decompilation, and/or Reverse Engineering of the software drivers for any purpose is strictly prohibited by international law. The copying of the software drivers, except for a reasonable number of back-up copies is strictly prohibited by international law. It is forbidden by international law to provide access to the software drivers to any person for any purpose other than processing the internal data for the intended use of the software drivers.

U.S. Government Restricted Rights Clause:
The software drivers are classified as "Commercial Computing device Software" and the U.S. Government is acquiring only "Restricted Rights" in the software drivers and their Documentation.

U.S. Government Export Administration Act Compliance Clause:
It is forbidden by US law to export, license or otherwise transfer the software drivers or Derivative Works to any country where such transfer is prohibited by the United States Export Administration Act, or any successor legislation, or in violation of the laws of any other country.

TRADEMARKS AND SERVICE MARKS

Inseego Corp. is a trademark of Inseego Corp., and the other trademarks, logos, and service marks (collectively the "Trademarks") used in this user manual are the property of Inseego Corp. or their respective owners. Nothing contained in this user manual should be construed as granting by implication, estoppel, or otherwise, a license or right of use of Inseego Corp. or any other Trademark displayed in this user manual without the written permission of Inseego Corp. or its respective owners.

- MiFi® and the MiFi logo are registered trademarks of Inseego Corp.
- Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

The names of actual companies and products mentioned in this user manual may be the trademarks of their respective owners.

Document Number: 14945410 *Rev 1*

Contents

1 Introduction 4
Overview 5
Key Features 5
Getting Support 5
2 Inseego Secure Dashboard 6
Overview 7
Signing In 7
Navigating the Interface 7
Tenant Dashboard 8
Events Dashboard 9
Devices Dashboard 10
Device Details Dashboard 11
Content Filtering Dashboard 17
Allowed List Tab 18
Blocked List Tab 18
Categories Tab 20
Notes on Caching 21

1

Introduction

Overview

Getting Support

Overview

Inseego Secure™ is a multi-layered, holistic security platform for Inseego IoT devices, providing proactive, real-time cybersecurity. Inseego Secure Agents operate on Inseego IoT devices, preventing, detecting, and responding to security breaches. The Inseego Secure Dashboard offers a cloud-based platform for viewing the data used and collected by Inseego Secure Agents, and setting up content filtering security options.

This guide describes the functions, capabilities, and options available on the Inseego Secure Dashboard.

Key Features

Inseego Secure provides:

- State of the art cyber protection with an AI-powered cloud engine that gathers complex event sequences and processes from your entire tenant of IoT devices - detecting network and operating system layer activities, leveraging behavioral-based analytics, and employing tenant-level security heuristics.
- Tenant risk visibility and protection, providing real-time vulnerability monitoring, real-time security hardening, and implementing CIS controls and benchmarks to provide global-standard security protections.
- Network and host intrusion detection and protection.
- 24/7 dedicated Security Operation Center (SOC) that conducts research, data analysis, and security event investigations, and offers 24/7 cybersecurity support.

Getting Support

Documentation for Inseego Secure is available online. Go to www.inseego.com/support-documentation.

For additional information and technical support, email Technical Support at technicalsupportus@inseego.com or call Customer Support (Toll Free) at **1-877-698-6481**.

2

Inseego Secure Dashboard

Overview

Tenant Dashboard

Events Dashboard

Devices Dashboard

Content Filtering Dashboard

Overview

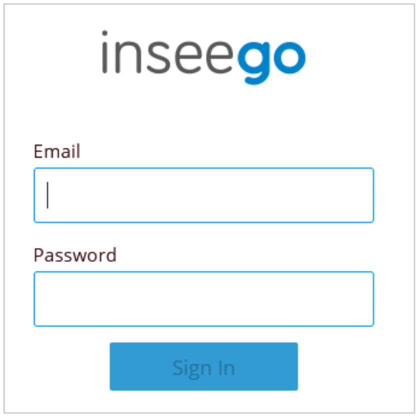
The Inseego Secure Dashboard is a Cloud-based user interface with access to the data used and collected by Inseego Secure Agents operating on your Inseego IoT devices.

You will receive an email with access information when your Inseego Secure account is created. If you have not received this email, be sure to check your spam folder or company filters.

Signing In

To sign in to Inseego Secure, go to https://secure.inseego.com.

The interface sign in screen appears:

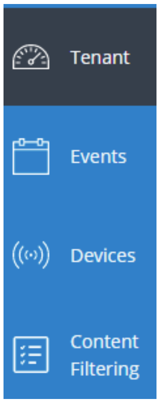


Enter the credentials supplied by your Inseego Secure contact and click **Sign In**.

The Tenant page of the Inseego Secure Dashboard displays.

Navigating the Interface

Use the side menu on the left of the page to access each page in the Inseego Secure Dashboard. You can use this menu to jump to other pages. The current page is indicated by a black highlight.

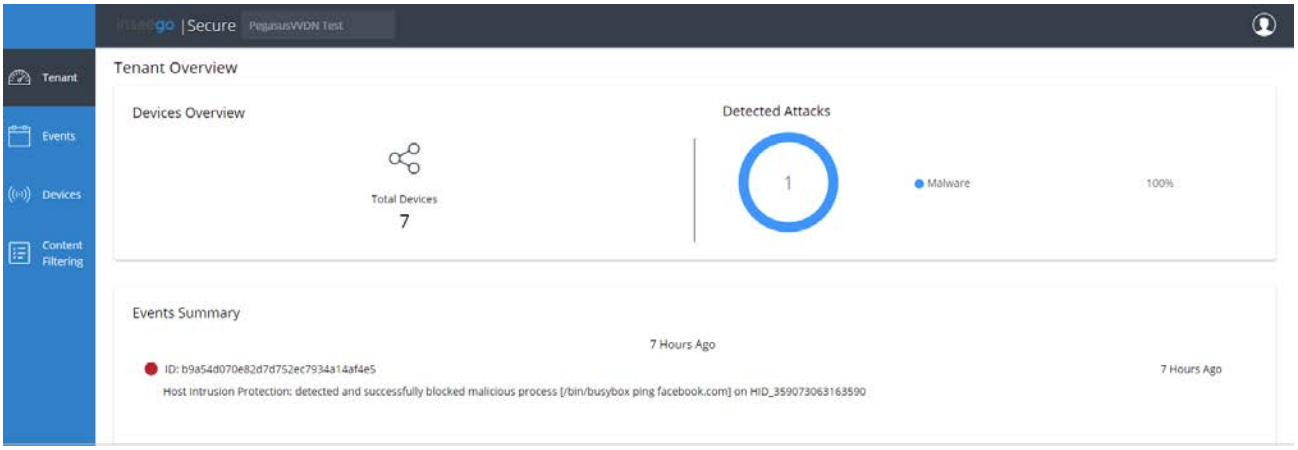


Click on the person icon 👤 in the upper right of any screen to change the tenant (if you belong to multiple tenants), or log out of Inseego Secure.

Tenant Dashboard

The Tenant page of Inseego Secure Dashboard provides an overview of devices and detected attacks, and a summary of security events for the devices in your tenant.

This page appears upon sign in. You can navigate to it from other pages by selecting **Tenant** from the side menu.



7 Hours Ago

● ID: b9a54d070e82d7d752ec7934a14af4e5 7 Hours Ago

Host Intrusion Protection: detected and successfully blocked malicious process [/bin/busybox ping facebook.com] on HID_359073063163590

Devices Overview

Displays the total number of devices in the tenant.

Detected Attacks

Displays the number of attacks against all devices in the tenant in the past 30 days and a breakdown of the type of attack (Malware, Malicious Connection, Brute Force, or Malicious Domain).

Events Summary

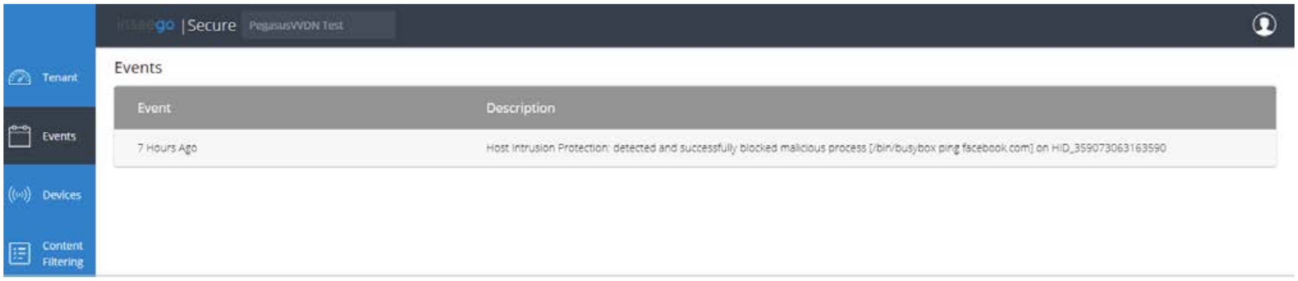
Displays all security events for devices in the tenant, including the ID and a description of the event, when the event occurred, and the ID of the device on which the event occurred.
Events are color coded by severity:

- 🟢 Green indicates the event is not associated with any malicious activity.
- 🟠 Amber indicates the event is identified as suspicious.
- 🔴 Red indicates an attack attempt was blocked.

NOTE: Click on the colored circle next to an event to launch the Events Dashboard.

Events Dashboard

The Events page on the Inseego Secure Dashboard displays security events for all devices in the tenant over the past 30 days. You can navigate to it from other pages by selecting **Events** from the side menu, or clicking on the colored circle next to an event.



Events

Event	Description
7 Hours Ago	Host Intrusion Protection: detected and successfully blocked malicious process [/bin/busybox ping facebook.com] on HID_359073063163590

Events

This table provides security event information on all devices in the tenant:

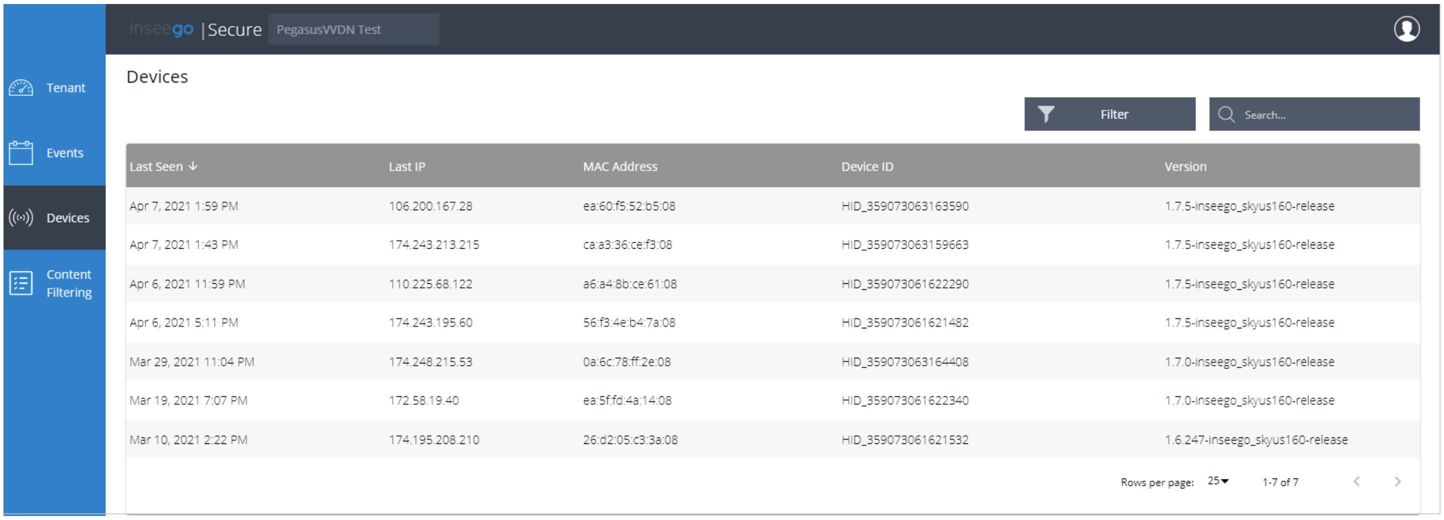
Event: Displays when the event occurred.

Description: A description of the event, including the ID of the device on which the event occurred.

Devices Dashboard

Use the Devices page on the Inseego Secure Dashboard to view information on all the devices in your tenant. You can navigate to it from other pages by selecting **Devices** from the side menu.

NOTE: You can click on a device row to access a device-specific dashboard that only displays information for that particular device (see Device Details Dashboard on page 11 for more information).



Devices

Last Seen ↓	Last IP	MAC Address	Device ID	Version
Apr 7, 2021 1:59 PM	106.200.167.28	ea:60:f5:52:b5:08	HID_359073063163590	1.7.5-inseego_skyus160-release
Apr 7, 2021 1:43 PM	174.243.213.215	ca:a3:36:ce:f3:08	HID_359073063159663	1.7.5-inseego_skyus160-release
Apr 6, 2021 11:59 PM	110.225.68.122	a6:a4:8b:ce:61:08	HID_359073061622290	1.7.5-inseego_skyus160-release
Apr 6, 2021 5:11 PM	174.243.195.60	56:f3:4e:b4:7a:08	HID_359073061621482	1.7.5-inseego_skyus160-release
Mar 29, 2021 11:04 PM	174.248.215.53	0a:6c:78:ff:2e:08	HID_359073063164408	1.7.0-inseego_skyus160-release
Mar 19, 2021 7:07 PM	172.58.19.40	ea:5f:fd:4a:14:08	HID_359073061622340	1.7.0-inseego_skyus160-release
Mar 10, 2021 2:22 PM	174.195.208.210	26:d2:05:c3:3a:08	HID_359073061621532	1.6.247-inseego_skyus160-release

Devices

This table provides information on all the devices in your tenant:

Last Seen: The date and time the device was last seen joining the network.

Last IP: The last IP address of the device.

MAC Address: The MAC Address (unique network identifier) for the device.

Device ID: The unique identifier for the device.

Version: The version of the Inseego Secure Agent that is running on the device.

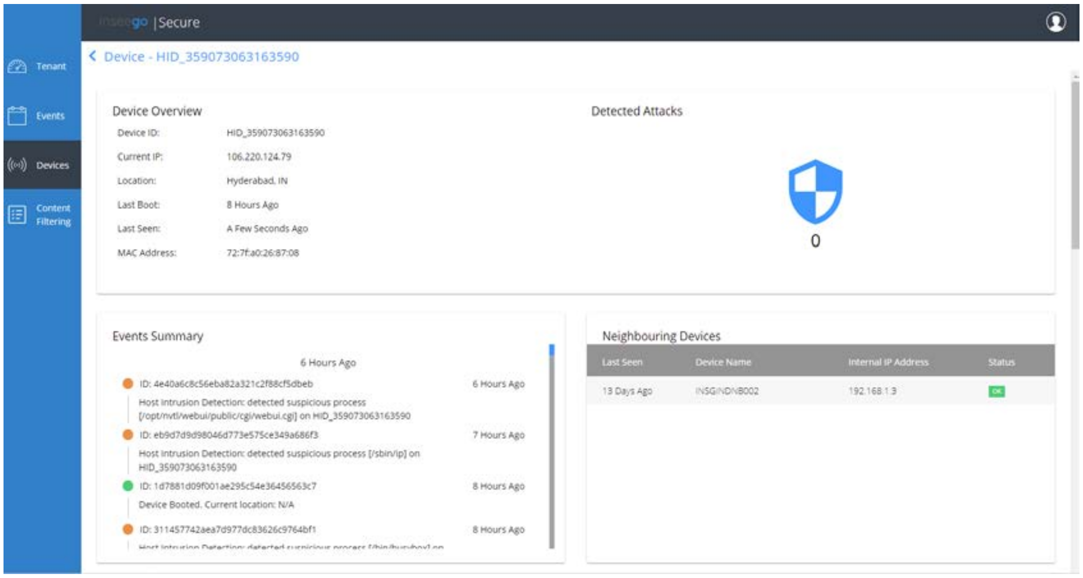
TIPS

▼ Use the Filter function in the upper right to display only devices that communicated within the time period you specify.

🔍 Use the Search box to search information on this page. Results appear as you type.

Device Details Dashboard

When you click on a device row in the Devices page, a dashboard with details for only that device appears.



Device - HID_359073063163590

Device Overview

Device ID:	HID_359073063163590
Current IP:	106.220.124.79
Location:	Hyderabad, IN
Last Boot:	8 Hours Ago
Last Seen:	A Few Seconds Ago
MAC Address:	72:7f:a0:26:87:08

Detected Attacks

0

Events Summary

6 Hours Ago

- ● ID: 4e40a6c8c56eba82a321c2f88cf5dbeb — 6 Hours Ago
  Host Intrusion Detection: detected suspicious process [/opt/nvtl/webui/public/cgi/webui.cgi] on HID_359073063163590
- ● ID: eb9d7d9d98046d773e575ce349a686f3 — 7 Hours Ago
  Host Intrusion Detection: detected suspicious process [/sbin/ip] on HID_359073063163590
- ● ID: 1d7881d09f001ae295c54e36456563c7 — 8 Hours Ago
  Device Booted. Current location: N/A
- ● ID: 311457742aea7d977dc83626c9764bf1 — 8 Hours Ago
  Host Intrusion Detection: detected suspicious process [/bin/busybox] on

Neighbouring Devices

Last Seen	Device Name	Internal IP Address	Status
13 Days Ago	INSGINDNB002	192.168.1.3	OK

Device Overview

The upper left section of this page provides information on the device similar to what is displayed on the Devices page.

Device ID: The unique identifier for the device.

Current IP: The last IP address of the device.

Location: The current location of the device.

Last Boot: When the device was last booted.

Last Seen: When the device was last seen joining the network.

MAC Address: The MAC Address (unique network identifier) for the device.

Detected Attacks

Displays the number of attacks against the device in the past 30 days**.**

Events Summary

Displays all security events for the device, including the ID and a description of the event, when the event occurred, and the ID of the device on which the event occurred.
Events are color coded by severity:

🟢 Green indicates the event is allowed by Inseego Secure.

🟠 Amber indicates the event is identified by Inseego Secure as suspicious.

🔴 Red indicates an attack attempt that was blocked.

NOTE: Click on the colored circle next to an event to launch the Events Dashboard.

Neighboring Devices

This list displays information on other devices identified on the same network, such as printers, routers, and other IoT devices.

Last Seen: When the device was last seen joining the network.

Device Name: The name of the device.

Internal IP Address: The IP address of the device for the local network.

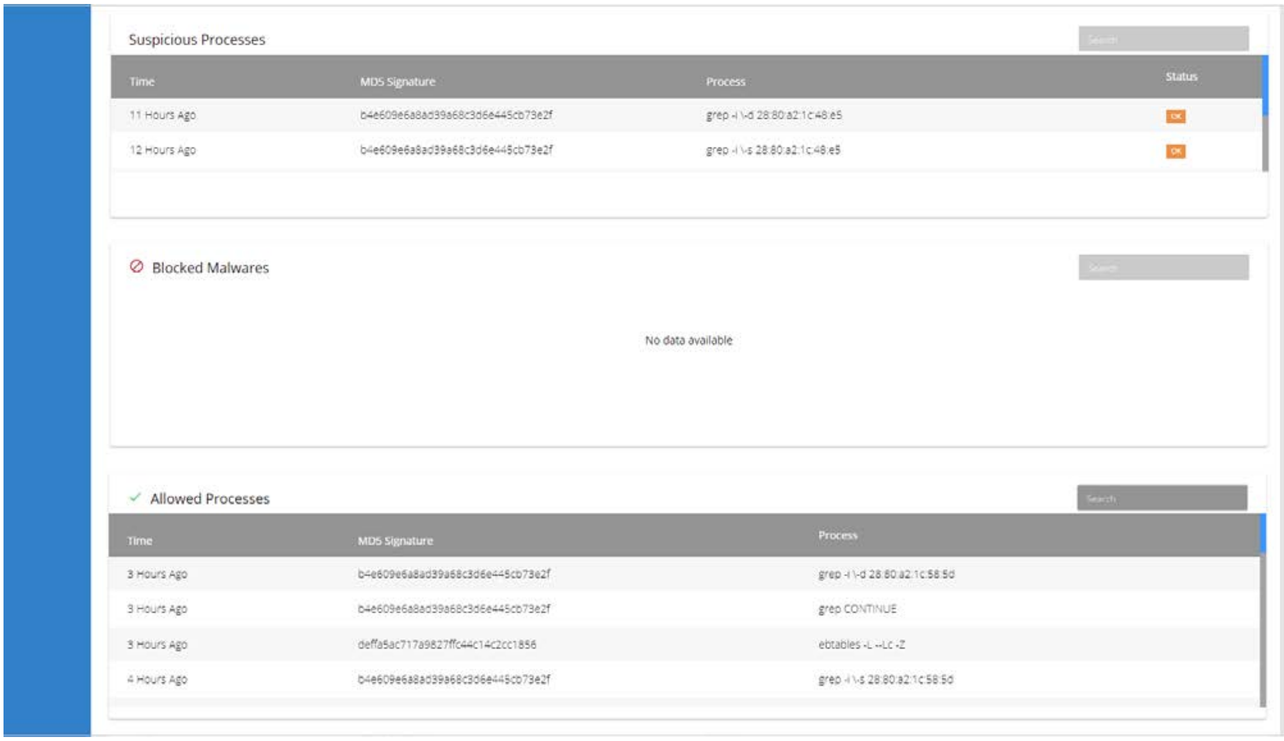
Status: The current security status of the device.

OK - The device is not associated with any malicious activity.

COMPROMISED - The device is conducting malicious activity.

BLOCKED - An attack attempt originating from the device was blocked.

NOTE: Scroll down to see more of the Device Details Dashboard.



Suspicious Processes

Time	MD5 Signature	Process	Status
11 Hours Ago	b4e609e6a8ad39a68c3d6e445cb73e2f	grep -i \-d 28:80:a2:1c:48:e5	OK
12 Hours Ago	b4e609e6a8ad39a68c3d6e445cb73e2f	grep -i \-s 28:80:a2:1c:48:e5	OK

Blocked Malwares

No data available

✓ Allowed Processes

Time	MD5 Signature	Process
3 Hours Ago	b4e609e6a8ad39a68c3d6e445cb73e2f	grep -i \-d 28:80:a2:1c:58:5d
3 Hours Ago	b4e609e6a8ad39a68c3d6e445cb73e2f	grep CONTINUE
3 Hours Ago	deffa5ac717a9827ffc44c14c2cc1856	ebtables -L --Lc -Z
4 Hours Ago	b4e609e6a8ad39a68c3d6e445cb73e2f	grep -i \-s 28:80:a2:1c:58:5d

Notes on Processes

The Inseego Secure Agent constantly monitors for the execution of new processes. For each new process creation, the Inseego Secure Agent sends the Inseego Secure Cloud data on the process (MD5, PID, path, process name and arguments, and PPID) for further processing.

Once the process data is received on the Cloud, the process is checked against the Inseego Secure internal Approved Processes list to verify that it is a legitimate process:

- If the process is on the Approved Processes list - the process is listed in the Allowed Processes table.
- If the process is ***not*** on the Approved Processes list, it is verified against the Threat Intelligence Engine (Antivirus database) to see if it is known to be malicious.
    - If the process is known to be malicious, a *kill* command is immediately pushed to the Agent to stop the execution of the process and the process is listed in the **Blocked Malwares** table. Once blocked, every instance of a process is automatically killed by the Inseego Secure Agent.
    - If the process is ***not*** known to be malicious, it is listed in the **Suspicious Processes** table for further human-based investigation by the Inseego Secure Security Operations Center (SOC).

Suspicious Processes

The Suspicious Processes table displays processes identified as suspicious by Inseego Secure. This includes all processes not on the Approved Process or not flagged as malicious.

Time: When the process occurred.

MD5 Signature: The MD5 hash associated with the process.

Process: The unique identifier of the process.

Status: The current status of the process.

OK - The process is not associated with any malicious activity.

TIP - Use the Search box in the upper right of the table to search records in this list.

NOTE: There is a learning period of a few days when Inseego Secure learns the device for the first time. During those first few days, no suspicious processes display. Once a process is listed in the Suspicious Processes table, the Inseego Secure Security Operations Center (SOC) investigates the process and approves or blocks it.

Blocked Malwares

The Blocked Malwares table displays processes either identified as malware or unauthorized to be executed. Once a process is on this list, every instance of that process will be automatically intercepted by the Inseego Secure agent on the device.

Time: When the process occurred.

MD5 Signature: The MD5 hash associated with the process.

Process: Unique identifier of the process.

TIP - Use the Search box in the upper right of the table to search records in this list.

NOTE: There is a learning period of a few days when Inseego Secure learns the device for the first time. During those first few days, no blocked processes display in the list.

Allowed Processes

The Allowed Processes table displays processes identified as allowed by Inseego Secure.

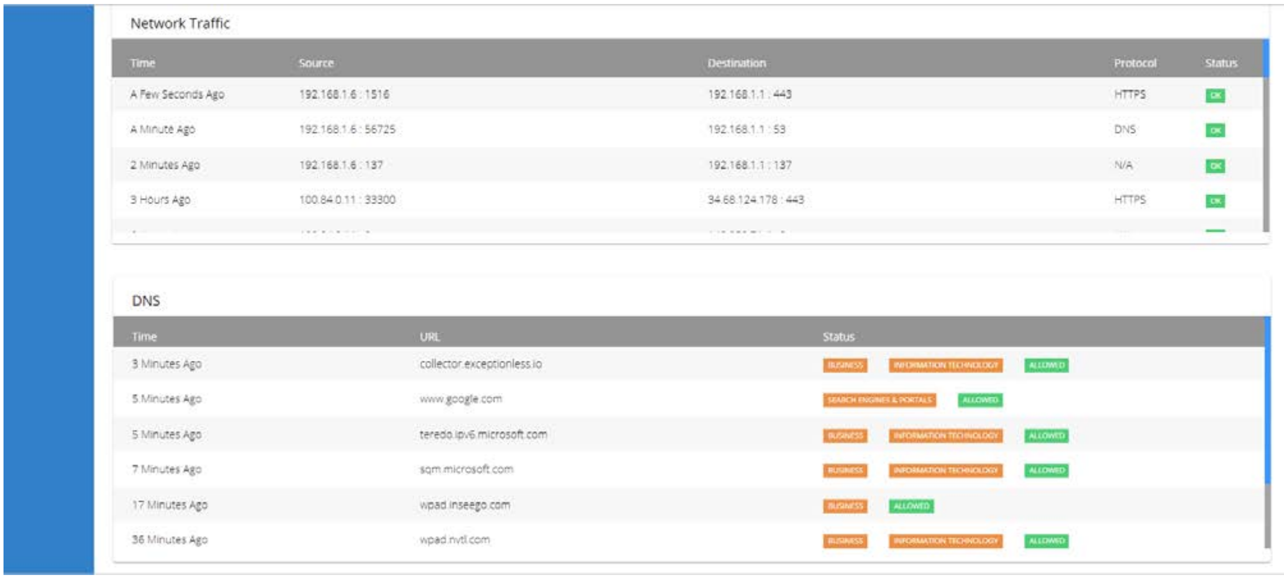
Time: When the process occurred.

MD5 Signature: The MD5 hash associated with the process.

Process: Unique identifier of the process.

TIP - Use the Search box in the upper right of the table to search records in this list.

NOTE: Scroll down to see more of the Device Details Dashboard.



Network Traffic

Time	Source	Destination	Protocol	Status
A Few Seconds Ago	192.168.1.6 : 1516	192.168.1.1 : 443	HTTPS	OK
A Minute Ago	192.168.1.6 : 56725	192.168.1.1 : 53	DNS	OK
2 Minutes Ago	192.168.1.6 : 137	192.168.1.1 : 137	N/A	OK
3 Hours Ago	100.84.0.11 : 33300	34.68.124.178 : 443	HTTPS	OK

DNS

Time	URL	Status
3 Minutes Ago	collector.exceptionless.io	BUSINESS INFORMATION TECHNOLOGY ALLOWED
5 Minutes Ago	www.google.com	SEARCH ENGINES & PORTALS ALLOWED
5 Minutes Ago	teredo.ipv6.microsoft.com	BUSINESS INFORMATION TECHNOLOGY ALLOWED
7 Minutes Ago	sqm.microsoft.com	BUSINESS INFORMATION TECHNOLOGY ALLOWED
17 Minutes Ago	wpad.inseego.com	BUSINESS ALLOWED
36 Minutes Ago	wpad.nvtl.com	BUSINESS INFORMATION TECHNOLOGY ALLOWED

Network Traffic

The Network Traffic table displays all traffic on the network by IP Addresses and port number, and indicates Inseego Secure analysis of the traffic.

Time: When the traffic occurred.

Source: The source IP address and port number.

Destination: The destination IP address and port number.

Protocol: The protocol associated with the traffic.

Status: The status of the traffic.

OK - The IP address is allowed.

BLOCKED – The IP address is blocked.

DNS

The DNS table displays all DNS queries originating from the device.

Time: When the DNS query occurred.

URL: The URL of the domain queried.

Status: The status of the query.

OK or **ALLOWED** - The domain is allowed or on the Content Filtering Allowed List.

CATEGORY – If the domain is associated with a category, the category name is shown.

MALICIOUS or **BLOCKED** – The domain is identified as associated with malicious activity, or is blocked by Content FIltering.

Content Filtering Dashboard

Use the Content Filtering page on the Inseego Secure Dashboard to define the domain access policy for all devices in your tenant. You can navigate to it from other pages by selecting **Content Filtering** from the side menu.

The Content Filtering page includes three tabs:

- Allowed List – use to allow access to specific domains.
- Blocked List – use to block access to specific domains.
- Categories – use to allow or block access to broad categories of domains.

IMPORTANT: There is an order of precedence to content filtering in Inseego Secure. It is helpful to remember that **the Allowed List always wins**.

1) **Allowed List** – Takes precedence over the Blocked List and Category blocks.
2) **Blocked List** – Takes precedence over domains allowed by Category.
3) **Categories** – Blocks or allows domains within categories only when those domains are not on the Allowed List or Blocked List.

NOTE: When a device with Inseego Secure first starts, it will take up to 60 seconds for content filtering to start running. During that time, browsing is allowed without filtering and DNS requests are not collected by Inseego Secure.

When a device experiences service failure or connectivity issues, such as ISP Internet connection problems, the Inseego Secure Agent blocks all DNS resolving services until a secured connection is restored in order to maintain enforced browsing. Recovering to a fully-secured, enforced connection may take 30 seconds to 60 seconds.

Notes on Adding Domain Names to Allowed or Blocked Lists

Domains are added to the Allowed List or Blocked List based on their Fully-Qualified Domain Name (FQDN), using the convention *subdomain.example.org*. Domains can be allowed or blocked at every level of the hierarchy:

- ***subdomain.example.org*** – Allows/blocks a particular subdomain.
- ***cnn.com*** – Allows/blocks *cnn.com* and all **.cnn.com* sub-domains, including *edition.cnn.com*.
- ***org*** – Allows/blocks all *.org* Top-Level Domains (TLDs).

NOTES:

- Adding a domain name, or Top-Level Domain (TLD) will block the domain and all subdomains, except for some sites where a subdomain is classified differently by Inseego Secure than the parent domain.
- **Do not add *www***. When you add a domain, Inseego Secure automatically also blocks the www subdomain. For example, if you add "facebook.com," "www.facebook.com" is also included. Including *www* functions as a subdomain-level block when a domain-level block is usually desired.
- When a domain resolves to a CNAME record instead of a record, Inseego Secure Agent performs a second lookup for the CNAME record (and continues looking for any nested

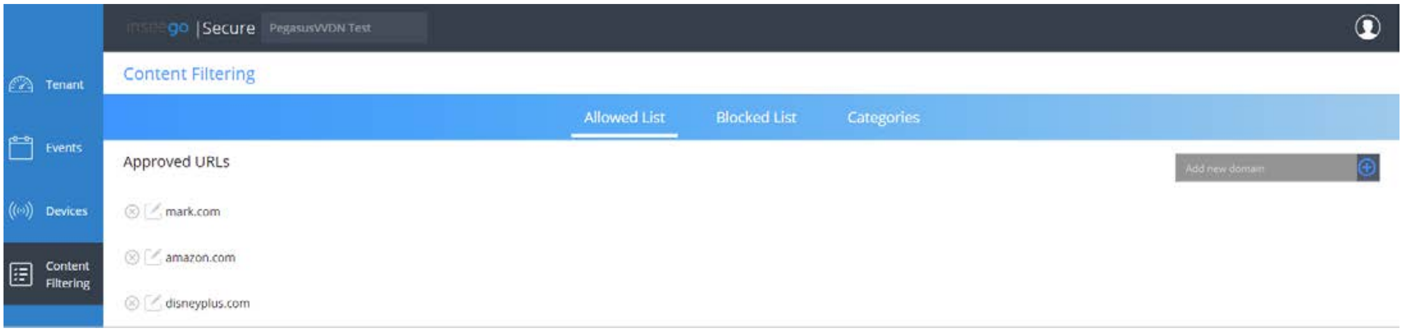
CNAME records). If any resulting CNAMEs are in a category that is blocked, the block page IP address is immediately returned instead of the CNAME record's actual value. Therefore, when adding a domain to the Allowed List, be sure to add all of the CNAMEs in the chain as well.

Domain Name Entries

Incorrect	Correct	Explanation
www.yahoo.com	yahoo.com	Do not include *www*. It is not necessary and blocks the www subdomain.
https://facebook.com	facebook.com	URLs are not accepted by Inseego Secure. Entries must be FQDNs.
198.251.90.71	example.org	Using IP addresses is not recommended, as they can change and filtering would be circumvented.
*.ru	ru	Top-level domains should be blocked simply based on their name (for example: ru, cn, tr). In this example, using *.ru would block all *.ru Russian domain space, including mail.ru.

Allowed List Tab

Use the Allowed List tab to view and add approved domains for all devices in your tenant.



Approved URLs

mark.com

amazon.com

disneyplus.com

Approved URLs

The Approved URLs list displays the URLs of domains that are approved for the devices in your tenant.

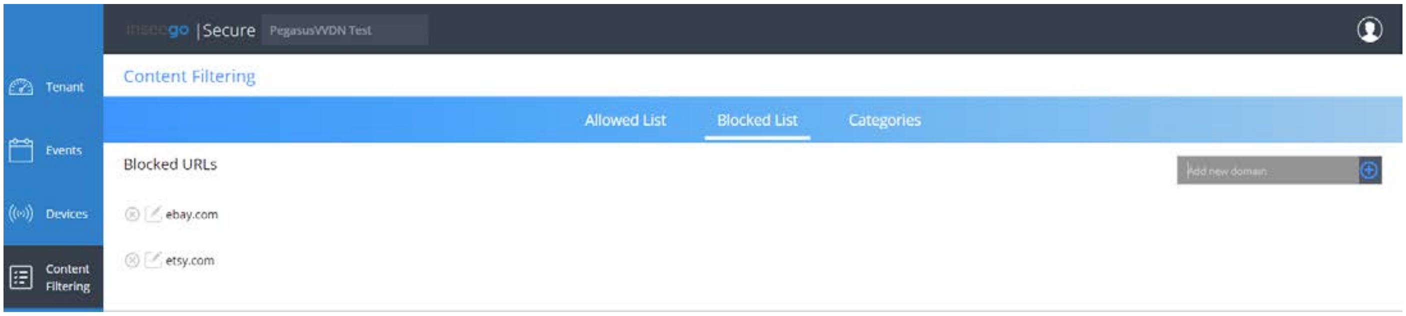
To add a new domain, type a URL into the **Add new domain** field in the upper right, then hit return or click the ⊕ add icon. The URL appears in the Approved URLs list.

To delete a domain, click the ⊗ delete icon next to the URL. The URL disappears from the list.

To edit a domain, click the ✎ edit icon next to the URL and edit the URL. Click the icon again when done.

Blocked List Tab

Use the Blocked List tab to view and add blocked domains for all devices in your tenant.



Blocked URLs

ebay.com

etsy.com

Blocked URLs

The Blocked URLs list displays the URLs of domains that are blocked for the devices in your tenant.

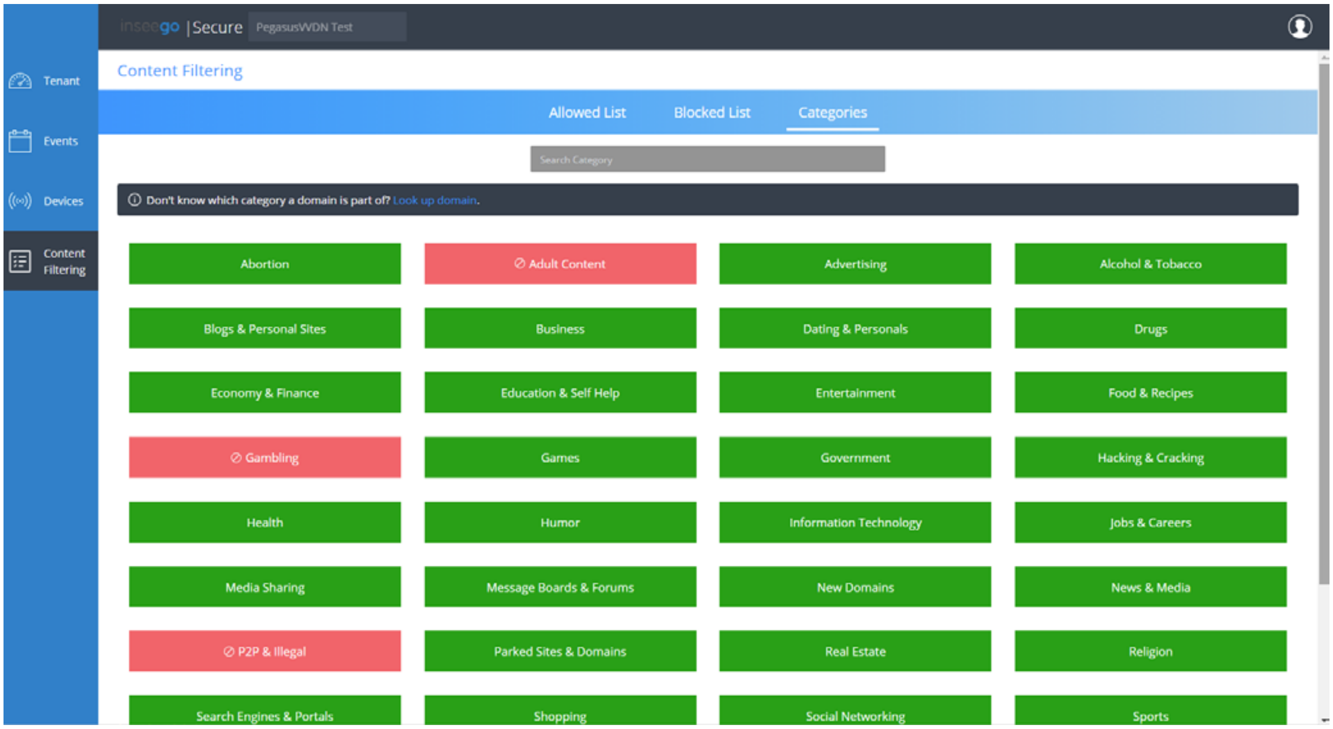
To add a new blocked domain, type a URL into the **Add new domain** field in the upper right, then hit return or click the ⊕ add icon. The URL appears in the Blocked URLs list.

To delete a domain, click the ⊗ delete icon next to the URL. The URL disappears from the list.

To edit a domain, click the ✎ edit icon next to the URL and edit the URL. Click the icon again when done.

Categories Tab

Use the Categories tab to block whole categories of undesirable domains. For example, blocking the Social Networking category blocks Facebook, Twitter, and Instagram.



ⓘ Don't know which category a domain is part of? Look up domain.

Abortion	⊘ Adult Content	Advertising	Alcohol & Tobacco
Blogs & Personal Sites	Business	Dating & Personals	Drugs
Economy & Finance	Education & Self Help	Entertainment	Food & Recipes
⊘ Gambling	Games	Government	Hacking & Cracking
Health	Humor	Information Technology	Jobs & Careers
Media Sharing	Message Boards & Forums	New Domains	News & Media
⊘ P2P & Illegal	Parked Sites & Domains	Real Estate	Religion
Search Engines & Portals	Shopping	Social Networking	Sports

To block or unblock a category, click the category. A blocked category appears red.

TIPS

Hover over a category for a description of the category.

Use the Search box at the top of the page to quickly search for a category.

To see what category a domain is part of, click **Look up Domain** and enter the URL.

Default Deny Filtering

Default Deny refers to the concept of blocking all possible domains by default, except those specified in the Allowed List. This is also referred to as "Allowed List only**"**.

Inseego Secure Dashboard does not have a single setting to enable Default Deny filtering, but you can achieve it by blocking all categories in the dashboard.

IMPORTANT: When setting up Default Deny filtering, keep in mind that adding a single domain to the Allowed List usually does not result in a fully functional website. Almost all websites use multiple domains and services to load content associated with the website. Inseego Secure Support is not able to assist with researching all the domains required to load a specific website or service with Default Deny filtering.

Notes on Caching

When you make content filtering changes on the Inseego Secure Dashboard, changes are reflected in the devices in your tenant instantly. However, DNS record information is usually cached (stored on your local browser, computer or network forwarder) for a specific amount of time; anywhere from five minutes to eight hours is normal.

Caching when Allowing Domains

When adding domains to the Allowed List, or removing categories from being blocked, changes are reflected in your network/computers within 30 seconds. Inseego Secure block pages have a 30-second cache time (TTL), so there should normally be no need to clear the cache on your computer or browser. However, some browsers and networking devices force a minimum cache time (TTL) of 60 seconds or more.

Caching when Blocking Domains

When adding domains to the Blocked List, or selecting additional categories to be blocked, affected domains may have been visited recently on computers in your network, and therefore the cache time (TTL) as set by the domain's DNS administrators could take minutes or hours to expire.

Clearing your Cache

If you are encountering issues with content filtering, such as blocking not working according to your Inseego Secure Dashboard specifications, clear both your system cache and browser cache.

On **Google Chrome (Windows and Mac)**:

1. In a new tab, type the following into the address bar and then click **Enter**:
   `chrome://net-internals/#dns`
2. Click **Clear host cache**.
3. Select **Sockets** from the left menu and click both **Close idle sockets** and **Flush socket pools**.