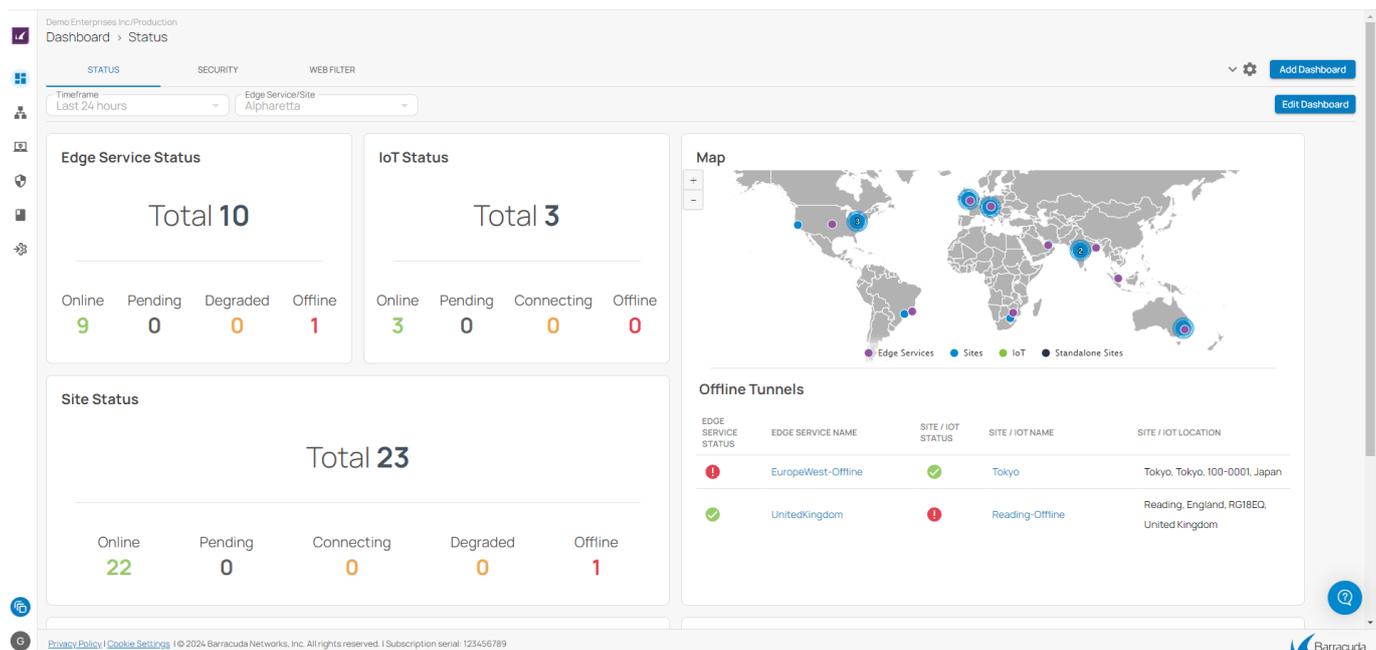


Dashboard

<https://campus.barracuda.com/doc/98223598/>

The Barracuda SecureEdge dashboard provides a comprehensive overview of SD-WAN connections, network activity, and traffic details, and shows actionable status and security information of connected sites. SD-WAN provides multiple VPN transports with each transport capable of using a different WAN connection, thereby expanding on the concept of a traditional VPN tunnel with only one VPN transport to one logical VPN tunnel. SD-WAN also provides redundant, reliable, and failsafe network connections: the VPN tunnel is up and can transmit traffic as long as at least one transport is operational. Admins can retain full control over how each transport is used, or they can configure the advanced balancing and bandwidth management features to optimally use the available bandwidth. For more information, see [SD-WAN Policies](#).

Barracuda SecureEdge explicitly provides information about SD-WAN tunnels.



The SecureEdge smart dashboard consists of four predefined, customizable pages: A general dashboard named **STATUS** provides information on the status of all connected devices, a dashboard named **SECURITY** displays information on security cards, a dashboard named **WEB FILTER** displays information on secure web gateway cards, and a dashboard named **ZERO TRUST ACCESS** provides information on the status of connected users, resources, and custom applications. You can perform the following on your smart dashboard:

- You can change the dashboard appearance as well as the displayed information per workspace.
- You can move (drag-and-drop) and modify each element as needed.

- You can create, modify, or delete your own customize dashboards and save them.

In the Barracuda SecureEdge Manager, a separate dashboard page is provided with more detailed information on each enrolled unit. This information is displayed in terms of various elements on the corresponding dashboard page. An enrolled unit can be an edge service, a site, or IoT devices.

STATUS Dashboard

The Barracuda SecureEdge **STATUS** dashboard provides an overview of all connections, and shows the network status, events, as well as the actionable status and security information of connected edge services, sites, and IoT devices. You can move (drag-and-drop) and modify each element according to your requirements. You can create, modify, or delete your own customize dashboards and save them.

The dashboard organizes information into elements and provides the following details:

Map

The appliance map provides a graphical view of active VPN tunnels and shows all connected sites, edge services, and IoT devices based on their geo-location.



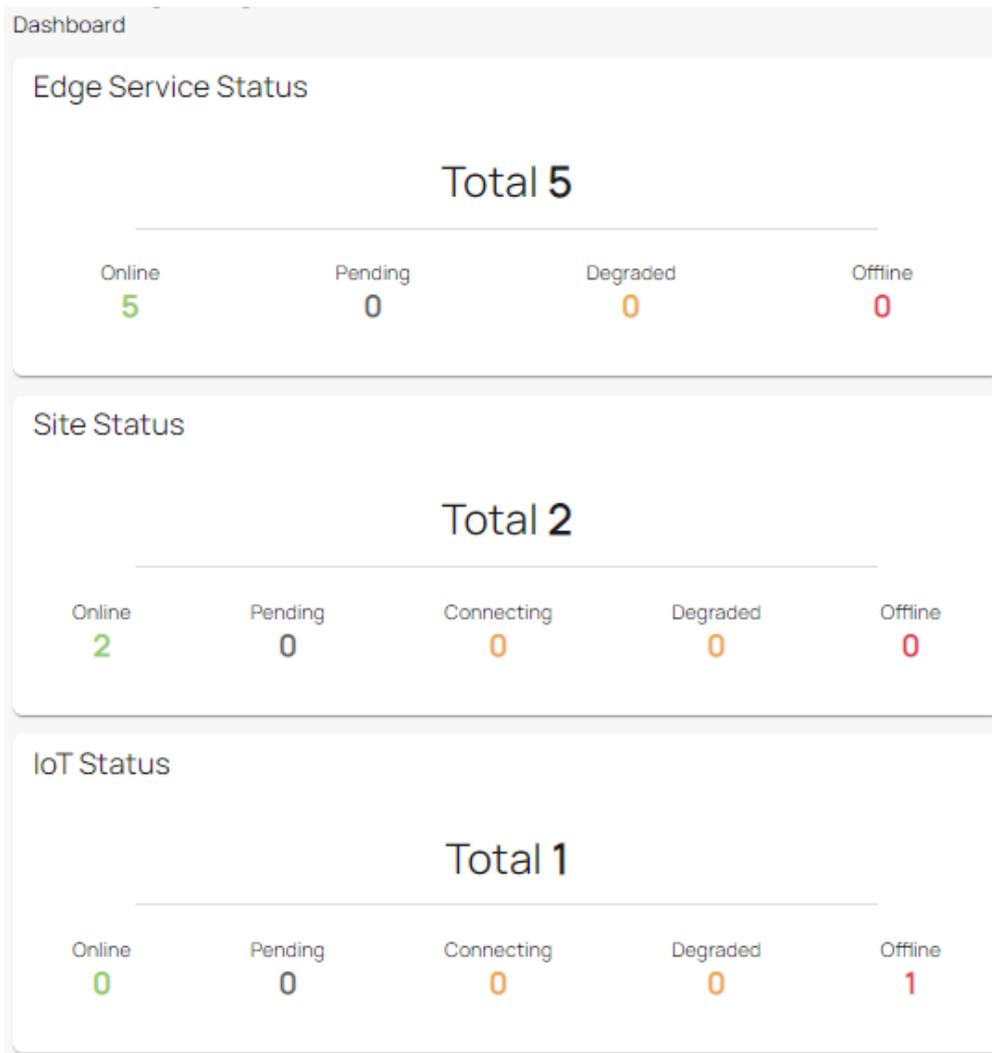
Click on a location to view more details for the connected site, service, or device.

Status of Edge Service, Site, and IoT

These elements list all connected edge services, sites, and IoT devices in total and provide information on the individual connection status. Enrolled units are shown in numbers with their status indicated by colors:

- **Online** – Edge service, site, or IoT device is up and running.

- **Pending** - Edge service, site, or IoT device is waiting for updates.
- **Connecting** - Edge service, site, or IoT device is trying to connect.
- **Degraded** - Connection is degraded.
- **Offline** - Connection is down.



To distinguish between the status of various enrolled units, different colors are used:

- **Green** - Connection to the appliance is online, and the appliance is up and running.
- **Yellow** - Connection to the appliance is degraded.
- **Orange** - Currently connecting to the appliance.
- **Gray** - Connection to the appliance is pending and waiting for updates.
- **Red** - Connected appliance is offline.

Events

The **Events** element provides details on recent events related to system status and administration.

Recent System Events		Recent Administrative Events	
✔ Update Setting	2023-11-17 07:09	✔ Update Zero Trust Settings	2023-11-17 07:10
✔ Update Setting	2023-11-17 07:09	✔ Update Zero Trust Settings	2023-11-17 07:10
✔ Update Setting	2023-11-17 07:09	✔ Configure VPN	2023-11-17 07:10
✔ Update Setting	2023-11-17 07:09	✔ Configure VPN	2023-11-17 07:09
✔ Update Setting	2023-11-17 07:09	✔ Create Malware Filter	2023-11-17 07:09

Offline Tunnels

The **Offline Tunnels** element provides information on all offline tunnels.

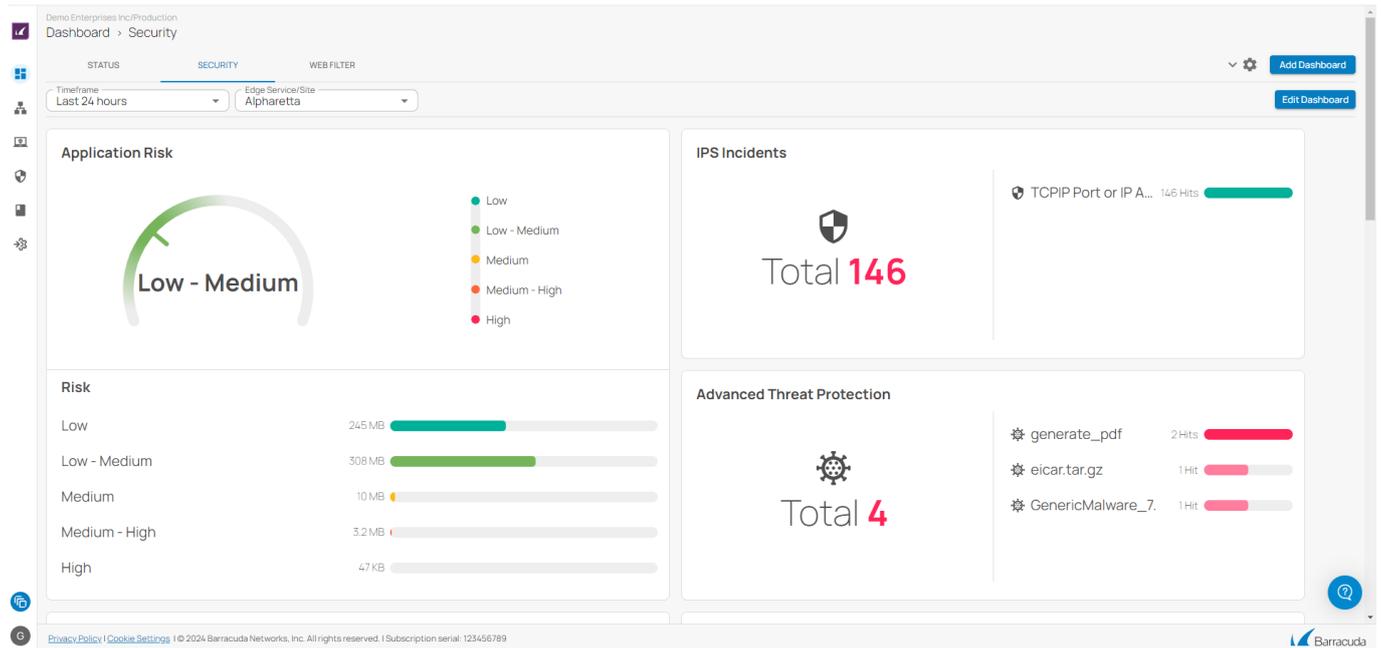
Offline Tunnels				
EDGE SERVICE STATUS	EDGE SERVICE NAME	SITE / IOT STATUS	SITE / IOT NAME	SITE / IOT LOCATION
!	EuropeWest-Offline	✔	Tokyo	Tokyo, Tokyo, 100-0001, Japan
✔	UnitedKingdom	!	Reading-Offline	Reading, England, RG18EQ, United Kingdom

Click on an entry to open the corresponding configuration window. For information on how to configure edge services, devices, and sites, see [Deployment](#) and [Getting Started](#).

SECURITY Dashboard

The Barracuda SecureEdge **SECURITY** dashboard displays security information. The security information can be added by adding various available widgets or cards. To access information on the security dashboard:

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to access information on the dashboard for.
3. Click **SECURITY DASHBOARD**.
4. The **Security** dashboard page opens. Specify the values for the following:
 - **Timeframe** - Select the desired time frame from the drop-down list. You can choose between **Last 24 hours**, **Last week**, **Last month**, or **Last 3 months**.
 - **Edge Service / Site** - Select the edge service or site from the drop-down list.
5. With respect to your desired time frame for a selected site or edge service, you can see a graphical representation of the status of all added security widgets/cards.



The elements on the SecureEdge **SECURITY** dashboard provide the following details:

- **Application Risk**
- **Risk**
- **IPS Incidents**
- **Advanced Threat Protection**
- **Top Blocked Applications**
- **Top Allowed Applications (per Traffic)**
- **Top Geo Destination Countries**
- **Top Allowed App Categories (per Traffic)**
- **Top Geo Source Countries**
- **Top Blocked Users**
- **Top Users**

WEB FILTER Dashboard

The Barracuda SecureEdge **WEB FILTER** dashboard provides information on secure web gateway cards/widgets. It also displays various top-traffic dashboard widgets such as allowed or blocked URL categories, allowed or blocked domains, and top users. To access information on the **WEB FILTER** dashboard:

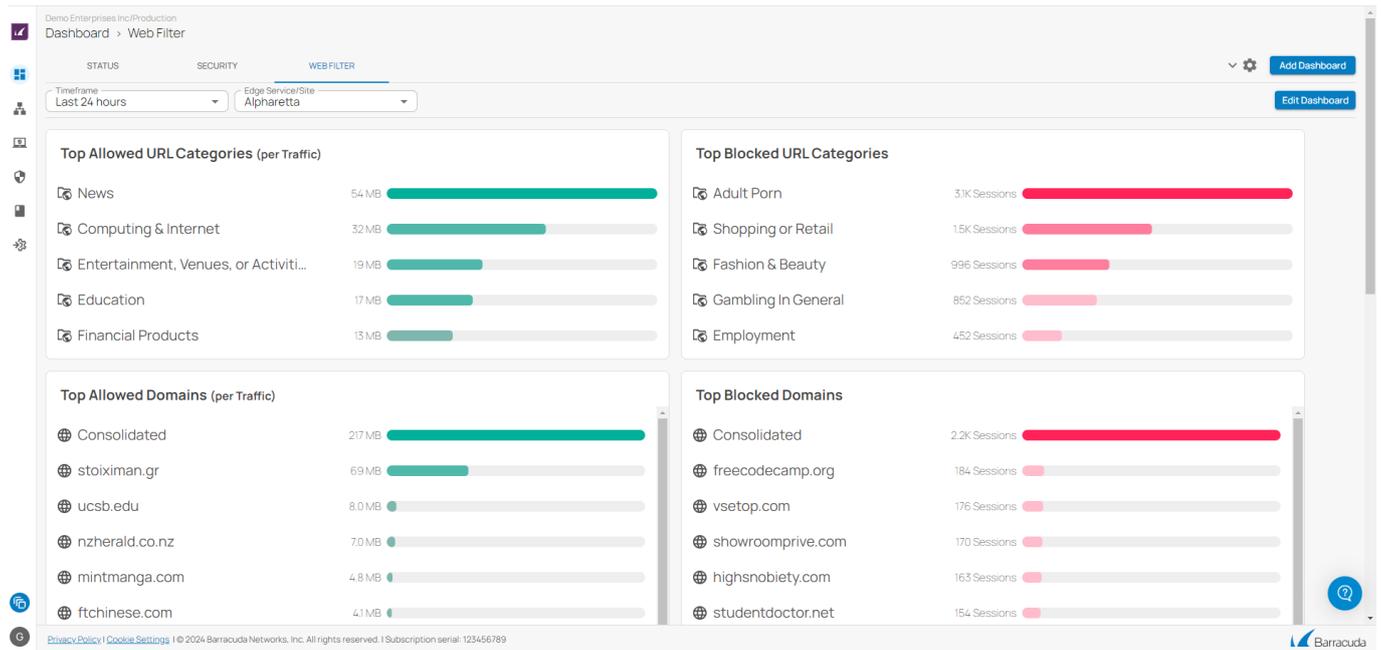
1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to access information on the dashboard for.

3. Click **WEB FILTER DASHBOARD**.

4. The **Web Filter** dashboard page opens. Specify the values for the following:

- **Timeframe** – Select the desired time frame from the drop-down list. You can choose between **Last 24 hours**, **Last week**, **Last month**, or **Last 3 months**.
- **Edge Service / Site** – Select the edge service or site from the drop-down list.

5. With respect to your desired time frame for a selected site or edge service, you can see a graphical representation of the status of all added widgets/cards.



The elements on the SecureEdge **WEB FILTER** dashboard provide the following details:

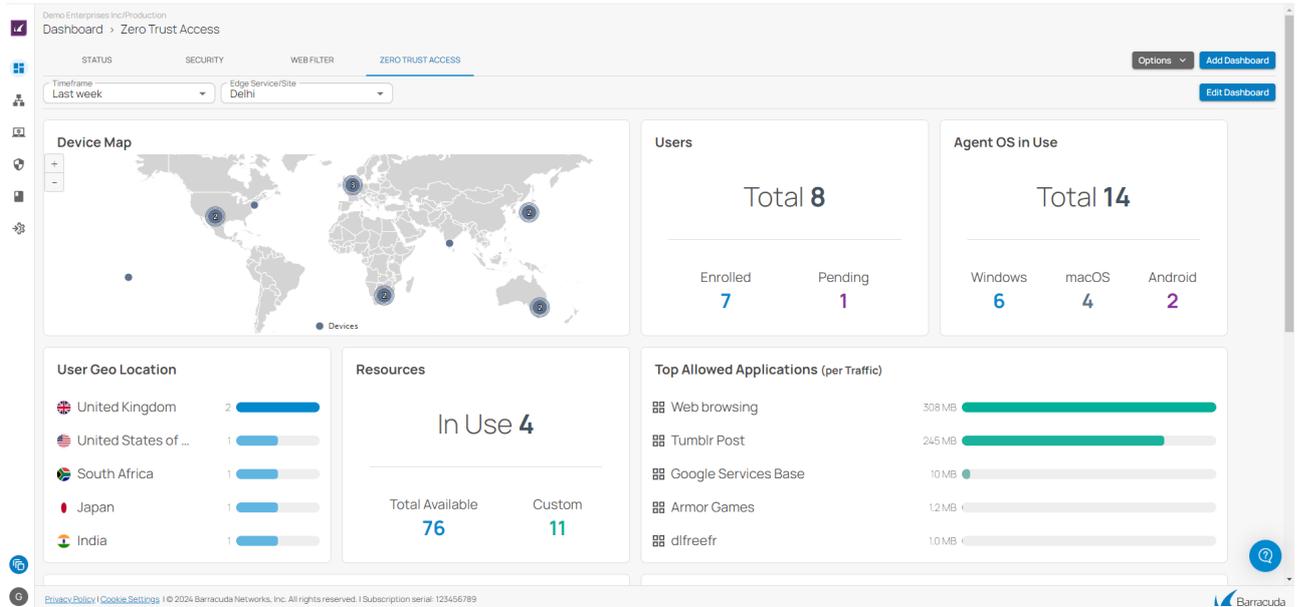
- **Top Allowed URL Categories (per Traffic)**
- **Top Blocked URL Categories**
- **Top Allowed Domains (per Traffic)**
- **Top Blocked Domains**
- **Top Users**
- **Top Blocked Users**

ZERO TRUST ACCESS Dashboard

The Barracuda SecureEdge **ZERO TRUST ACCESS** dashboard displays information on the status of connected users, resources, and custom applications. The Zero Trust Access information can be added by adding various available widgets or cards. To access information on the ZTA dashboard:

1. Go to **Dashboard > ZERO TRUST ACCESS**.
2. The **Zero Trust Access** dashboard page opens. Specify the values for the following:

- **Timeframe** – Select the desired time frame from the drop-down list. You can choose between **Last 24 hours**, **Last week**, **Last month**, or **Last 3 months**.
 - **Edge Service / Site** – Select the edge service or site from the drop-down list.
3. With respect to your desired time frame for a selected site or edge service, you can see a graphical representation of the status of all added widgets/cards.



The elements on the SecureEdge **ZERO TRUST ACCESS** dashboard provide the following details:

- **Users**
- **Agent OS in Use**
- **User Geo Location**
- **Resources**
- **Top Allowed Applications (per Traffic)**
- **Top Allowed URL Categories (per Traffic)**
- **Top Allowed Domains (per Traffic)**
- **Agent Version in Use**
- **Top Version in Use**
- **Device Map**

For more information, see [How to Customize a SecureEdge Zero Trust Access Dashboard](#).

Additional Information

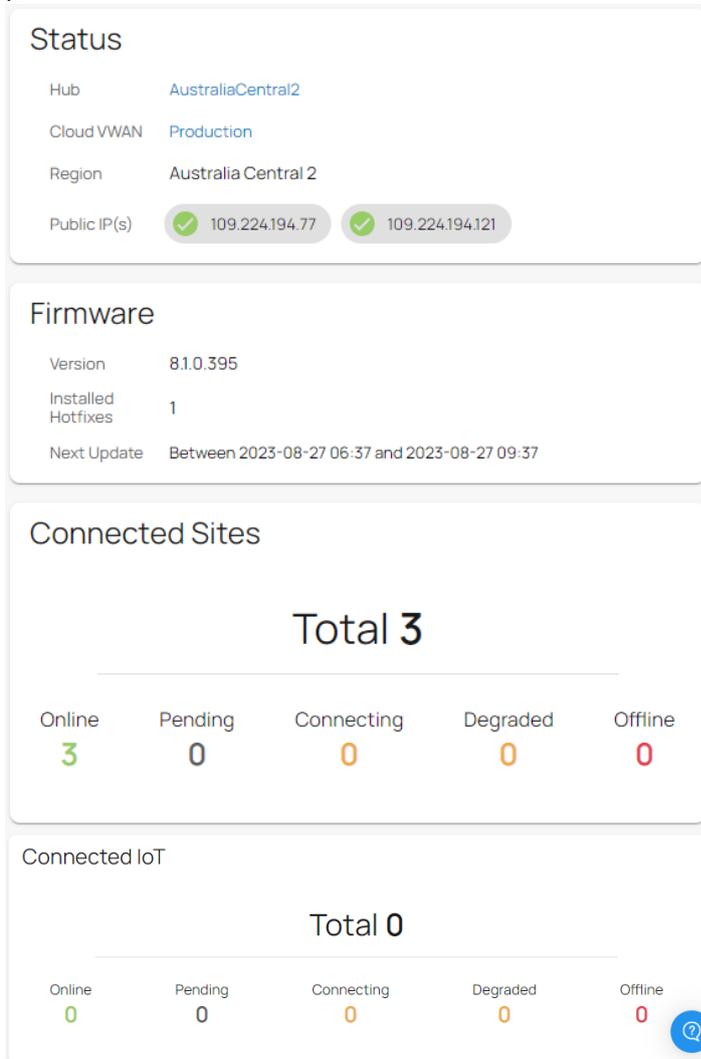
Accessing Information on the Edge Services Dashboard

The SecureEdge **Edge Services** page gives you an overview of all connected edge services for virtual WAN and private edge. The edge service for the virtual WAN dashboard provides aggregated data on each element of the connected edge service, such as status, firmware, and connected sites and IoT

devices.

To access the edge service for the **Virtual WAN** page, select your workspace, go to **Infrastructure > Edge Services** and click on the arrow icon next to the edge service you are interested in. The **Edge Service Dashboard** page provides following details:

- **Status** - The Status element displays the status of the connected edge service for Virtual WAN.
- **Firmware** - The Firmware element displays the installed software version and hotfixes, and provides the time period for the next updates.
- **Connected Sites** - The Connected Sites element displays all connected sites in total and provides information on the individual connection status.
- **Connected IoT** - The Connected IoT element displays all connected IoT devices in total and provides information on the individual connection status.



The screenshot displays the Edge Service Dashboard with the following sections:

- Status:** Hub: AustraliaCentral2; Cloud VWAN: Production; Region: Australia Central 2; Public IP(s): 109.224.194.77, 109.224.194.121 (both with green checkmarks).
- Firmware:** Version: 8.1.0.395; Installed Hotfixes: 1; Next Update: Between 2023-08-27 06:37 and 2023-08-27 09:37.
- Connected Sites:** Total 3. Status breakdown: Online (3), Pending (0), Connecting (0), Degraded (0), Offline (0).
- Connected IoT:** Total 0. Status breakdown: Online (0), Pending (0), Connecting (0), Degraded (0), Offline (0). A blue question mark icon is visible in the bottom right corner of this section.

To access the **Private Edge** page, select your private Edge Service and repeat the corresponding steps. The **Private Edge** dashboard displays more elements in addition to the elements listed above.

These elements are as follows:

- **Licenses** – The Licenses element displays information on the status of current licenses.
- **Hotfixes** – The Hotfixes element displays the status of current hotfixes for each connected private edge.
- **Configuration Updates** – The Configuration Updates element displays details about your configuration updates.
- **Services** – The Services element displays the status of services running on your private edge.
- **Interfaces** – The Interfaces element displays the status of network interfaces connected to your private edge.
- **Resources** – The Resources element displays details about the real-time usage of your system's resources.
- **VPN Tunnels** – The VPN Tunnels element displays the status of all VPN tunnels connected to your private edge.

Accessing Information on the **SITE** Dashboard

The SecureEdge **SITE** dashboard provides a comprehensive overview of each element of a connected site or sites.

To access the SecureEdge **Site** page, first select your workspace, go to **Infrastructure > Sites**, and click on the arrow icon next to the site you are interested in. The SecureEdge **Site Dashboard** page provides following details:

- **Status** – The Status element displays the status of the connected site or sites.
- **Licenses** – The Licenses element displays information on the current status, state, serial number, type, and expiration date of your licenses.
- **Edge Service** – The Edge Service element displays information on each connected edge service.
- **Firmware** – The Firmware element displays the installed software version and hotfixes, and provides the time period for the next update of your site or sites.
- **Hotfixes** – The Hotfixes element displays the status of current hotfixes for your connected site or sites.
- **Configuration Updates** – The Configuration Updates element displays information on configuration updates, such as last update, last seen, and your remote IP.

Status

Model: VT3000

Serial(s): ✔ 752124

Licenses

STATUS	SERIAL	STATE	TYPE	EXPIRATION DATE
✔	752124	Licensed	BYOL	2024-05-24 10:41

Edge Service

Name: UnitedStates

Cloud VWAN: Production

Hub: NorthAmerica

Region: West US

Size: 20 Scale Units - 10.0 Gbps

Firmware

Version: 8.1.0.395

Installed Hotfixes: 1

Next Update: Between 2023-08-14 04:52 and 2023-08-14 07:52

Hotfixes

STATUS	NAME
✔	Hotfix 1025 - Traffic flow influenced by URL Filter Application Rule
?	Hotfix 1027 - Cumulative Update for CGF 8.0.3

Configuration Updates

Last Update: 2023-05-14 03:51

Last Seen: 2023-05-24 10:43

Remote IP: 112.42.53.12

- **Services** - The Services element displays the status of all available services running on the connected site, such as SD-WAN, configuration, routing, firewall, IPS, and URL filtering.

Services

-  SD WAN ✔ OK
-  Configuration ✔ OK
-  Routing ✔ OK
-  Firewall ✔ OK
-  IPS ✔ OK
-  URL Filtering ✔ OK

- **Interfaces** - The Interfaces element provides an overview on the status of all network interfaces connected to your sites.

Interfaces				
STATUS	NAME	SPEED	DUPLEX	ERRORS
✓	IT	1 Gbps	Full	0
✓	Engineering	1 Gbps	Full	0
✓	Comcast	1 Gbps	Full	0
✓	Century-Link	1 Gbps	Full	0
✓	AT-And-T	1 Gbps	Full	0

- **Resources** - The Resources element provides information on the overall real-time usage of your system's resources. This element displays, as a percentage, the system load (CPU Load) and the amount of RAM (memory usage) used and still available. Hover over each resource to see the exact figures for used and available system resources. The following information is provided:
 - **CPU** - Displays the current CPU load of the connected site.
 - **Memory** - Displays the real-time usage of RAM.
 - **Hard disk** - Displays the real-time usage of all currently mounted file systems.
 - **/art** - Directory for basic system configurations and recovery operations. Displays the used and available ART disk space.
 - **/boot** - Directory for boot images. Displays the used and available boot disk space.
 - **/phion0** - Directory for logs and statistical data. Displays the used and available space.
 - **/** - Root directory. Displays the used and available space.



- **VPN Tunnels** - The VPN Tunnels element displays the status of all VPN tunnels connected to your sites.

VPN Tunnels				
STATUS	NAME	PEER	LOCAL	TYPE
✓ Up	wanhub-S20	109.224.194.62	172.16.107	TINA Site-2-Site

Accessing Information on the IoT Dashboard

The SecureEdge **IoT** dashboard provides aggregated data on each element of a connected IoT device.

To access an IoT page, first select your workspace, go to **Infrastructure > IoT** and click on the arrow icon next to the IoT device you are interested in. The **IoT Dashboard** page provides the following details:

- **Status** - The Status element displays the status of a connected IoT device.
- **Edge Service** - The Edge Service element displays information on each connected edge service.
- **Firmware** - The Firmware element displays the installed software version and provides the time period for next update for your connected IoT device.
- **Configuration Updates** - The Configuration Updates element displays information on configuration updates for your connected IoT device, such as last update and last seen.

<h3>Status</h3> <p>Model FSC2.9</p> <p>Serial ✔ 230111</p>	<h3>Firmware</h3> <p>Version 8.1.0.395</p> <p>Next Update Between 2023-08-12 16:24 and 2023-08-12 19:24</p>
<h3>Edge Service</h3> <p>Name Austria</p> <p>Cloud VWAN Production</p>	<h3>Configuration Updates</h3> <p>Last Update 2023-04-26 04:32</p> <p>Last Seen 2023-05-24 14:46</p>

Figures

1. status-dashboard.png
2. image2022-8-26 11:48:20.png
3. stat_01.png
4. RecentSystemEvents.png
5. RecentAdminEvents.png
6. off-tunnels.png
7. security-db.png
8. webfilter-db.png
9. db_zero_trust_access.png
10. status-fw-sites.png
11. conn-IoT.png
12. site-status.png
13. hotfixes-status.png
14. services-9.0.png
15. interfaces-site.png
16. resources-9.0-site.png
17. vpn-tunnels.png
18. status-iot.png
19. firmware-iot.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.