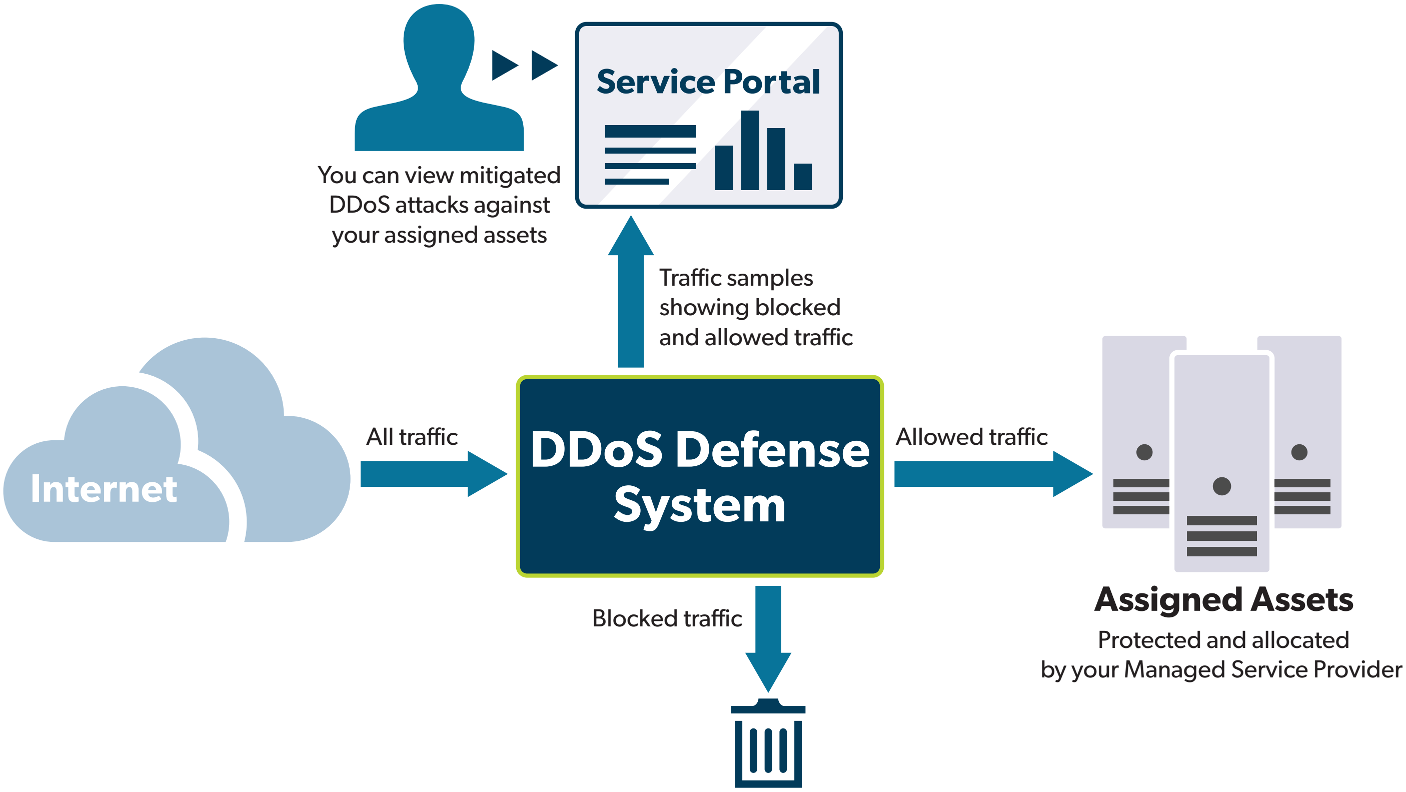
FirstLight®

DDoS Portal User Guide

Table of Contents

FirstLight DDoS Service Portal

The FirstLight DDoS Service Portal enables you to view and analyze DDoS attacks against your protected assets from a browser. You can use it to understand how many attacks you are being protected from, when they occurred, and what type of attack vector was detected. You can also use the portal to see ongoing attack mitigation, in real time.


Service Portal
You can view mitigated DDoS attacks against your assigned assets
Traffic samples showing blocked and allowed traffic
Internet
All traffic
DDoS Defense System
Allowed traffic
Blocked traffic
Assigned Assets
Protected and allocated by your Managed Service Provider

Working in the Service Portal

You can access the Service Portal from any of the following supported web browsers:

- **Chrome:** 71 or newer
- **Edge:** 44 or newer
- **Firefox:** 64 or newer
- **Safari:** 12 or newer
- **Internet Explorer:** not supported

The main navigation is from the main toolbar at the top of each screen. On the left of the main toolbar, you have the portal user functions and, on the right, you have system settings and account options.

Some of the portal screens such as System, also include tabs which enable you to switch between additional views.

Any fields which require input will be indicated inline, with other warnings indicated by a notification panel which appears temporarily in the bottom right corner of the screen, explaining the issue. If everything is working as expected, but there is no data to display in a table or chart, you will see a message such as "No data in this period."

Getting Started

Once you have access to the FirstLight Service Portal you should first log in and change your password. Administrative users can then start to configure the Service Portal for your organization.

Logging In to the Service Portal

Once you receive login credentials from FirstLight, you can access the Service Portal via the login page.

> **Caution:** You are only allowed three failed login attempts before you must reset your password.

To log in to the Service Portal

1. In a browser, navigate to the web address you were given by your provider.
2. Type in your **Username** and **Password**.
3. Click **Log in**.
4. The Service Portal opens on the Service Overview screen.

To log out of the Service Portal

1. On the far right of the main toolbar, click your account username.
2. From the drop-down, select **Log Out**.

Changing your own Password

When you first access the FirstLight Service Portal you will be using the default password provided with your account. You should change your password at the first opportunity. You will be prompted to change your password after a period of time set by FirstLight.

If you later forget your password, you can reset it using a Reset Token sent to your registered email address.

> **Note:** A password must be at least 8 characters long; including 1 number, 1 lowercase character, 1 uppercase character and 1 special character from the following list: $@#!%*?&^-_~.:(){}[]?.

To change your password from inside the Service Portal

1. On the right of the main toolbar of the Service Portal, click your account username.
2. From the drop-down, select **Change Password**.
3. Type your **Old Password**.
4. Type your new password in both the **New Password** and **Confirm Password** fields.
5. Click **Update Password**.
6. The next time you log in, you can now use the new password.

To recover your password using email verification

1. At the log in screen, click **Password Recovery**.
2. In the Forgot Password field, type in the email address for your account.
3. Click **Send Email**.
4. When you receive the password reset email it will contain a Reset Token
5. Return to the Password Recovery screen of the Service Portal in a browser.
6. In the Token field, enter your Reset Token.
7. Click **Reset Password**.
8. Type in your new password in both fields and click **Update Password**.
9. You can now log in to the Service Portal with your new password.

Editing your own User Profile

While Administrators are able to edit all users' details, every user is able to keep their own profile information up to date.

To edit your user profile

1. On the right of the main toolbar of the Service Portal, click your account username.
2. From the drop-down, select **Edit Profile**
3. You can edit the following details:
    - **First Name** and **Last Name**
    - **Phone** number
    - **Timezone**
4. You can choose to suppress emails by checking the boxes next to any of the following:
    - **Service level status alerts**
    - **Attack status alerts**
    - **Service overview reports**
    - **Per tenant reports**
5. Click **Save**.

Tip: Administrators can also edit a user's details at **System** > **Users**.

Configure the Service Portal

> **Note:** Configuring the Service Portal must be performed by a Tenant Administrator. If you are a Tenant User, skip to Service Overview and Attack Analysis.

FirstLight will have configured the basic settings for your DDoS Service Portal by adding the list of assets that are covered by the DDoS protection service, and by creating at least one Tenant Administrator account. As a Tenant Administrator, you can now further configure those features for your organization:

- Managing assets
- Creating asset groups
- Creating user accounts for your colleagues

In addition to Tenant Administrators, you can create Tenant User accounts that can view attacks and view the asset list, but not make any changes.

> **Note:** When you create a named item in the Service Portal (e.g. adding an asset name), there is a 255 character limit.

Users Overview

Users can access the FirstLight Service Portal using their individual account credentials. Initially, there will be at least one Tenant Administrator account, created for you by the provider. A Tenant Administrator can create additional users for the tenancy, which can be Tenant Administrators or Tenant Users:

- **Tenant Administrator** – Can view traffic data, analyze attacks, manage assets, and manage other Tenant Administrators and Tenant Users
- **Tenant User** – Can view traffic data, analyze attacks and view the asset list

Alerts

FirstLight can choose to send emails to users when an event occurs which they may need to be aware of. For each type of alert they can choose to send an email to Tenant Administrators, Tenant Users, or both.

- **Service level alerts** – FirstLight sends an email when you exceed your service level's maximum mitigation rate
- **Attack status alerts** – FirstLight sends an email when an attack occurs against one of your assets

> **Note:** You can choose to suppress alerts for specific users if you don't want them to receive these alert emails.

Reports

FirstLight can send out reports on a regular basis which summarize all the mitigated attacks against your assets, in a set time period. The reports are created as PDFs and will be sent out to users' registered email addresses. FirstLight can choose to send this report to Tenant Administrators, Tenant Users, or both.

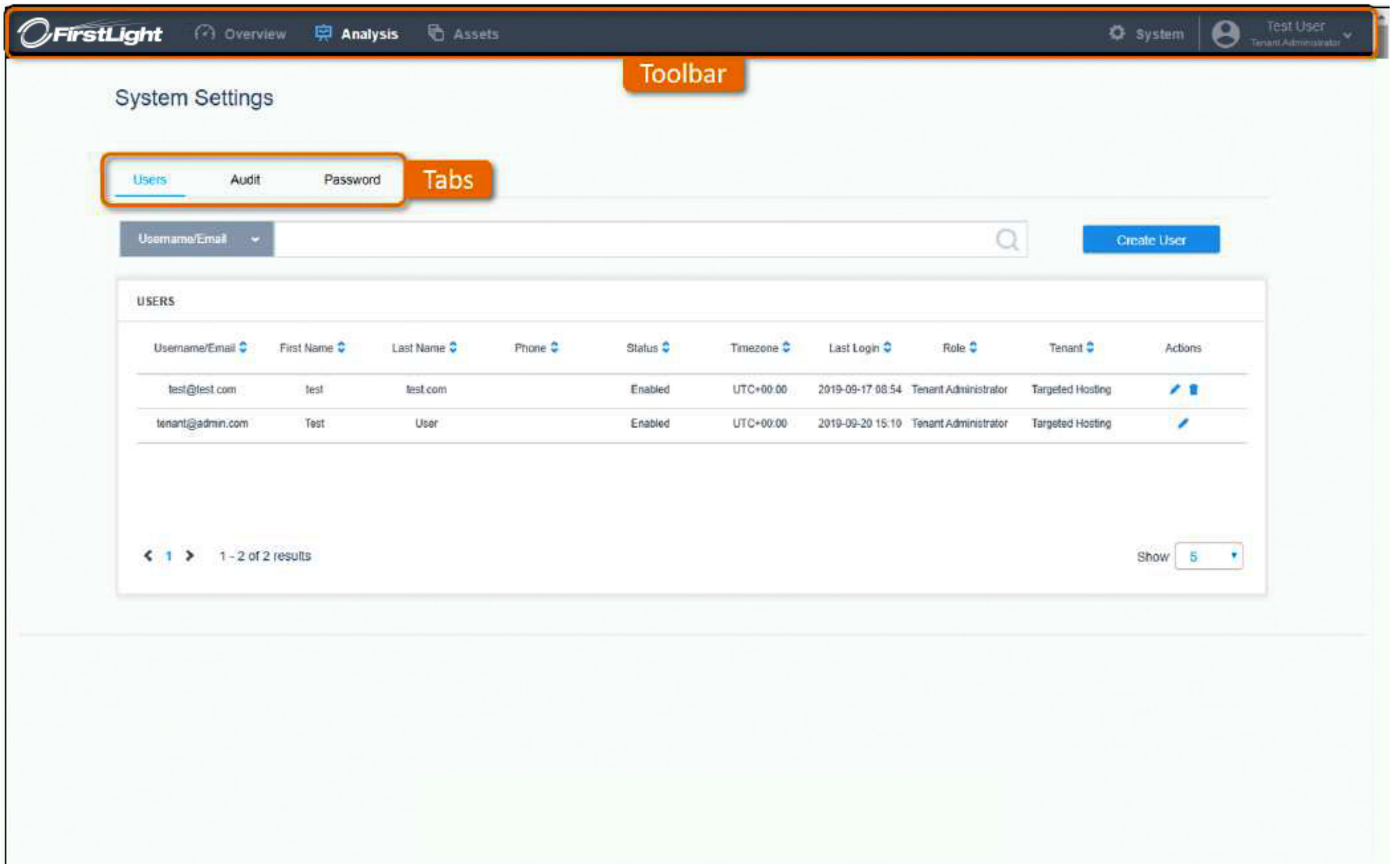
> **Note:** You can choose to suppress reports for specific users if you don't want them to receive these report emails.

Passwords

For security reasons, all users in the Service Portal must reset their password after a set period of time. Before their password expires, users should receive a notification of their upcoming expiration day and instructions to change the password using the **Change Password** feature in the Account drop-down or the **Forgot Password?** link on the log in screen. If they do not change their password before the expiration date, they will be unable to access the Service Portal and must contact their administrator or FirstLight to change their password.

Users Settings Screen

You can navigate to the Users tab of the System Settings Screen by clicking **System** on the main toolbar.



Username/Email	First Name	Last Name	Phone	Status	Timezone	Last Login	Role	Tenant	Actions
test@test.com	test	test.com		Enabled	UTC+00:00	2019-09-17 08:54	Tenant Administrator	Targeted Hosting	
tenant@admin.com	Test	User		Enabled	UTC+00:00	2019-09-20 15:10	Tenant Administrator	Targeted Hosting	

The **Search** bar and drop-down at the top of the users screen enables you to search for specific attacks. You can select one of the following categories and type a search term:

- **Username/Email** – Select this option then type all or part of an email address to view only users whose email address matches the search term. For example, you can filter to only show users who use company email addresses by typing the last half of an email (i.e. @company.com).
- **First Name** – Select this option then type all or part of a first name to view only users whose first name matches the search term
- **Last Name** – Select this option then type all or part of a last name to view only users whose last name matches the search term
- **Phone** – Select this option then type all or part of a phone number to see users that match that number
- **Status** – Select this option then type **Enabled** or **Disabled** to filter the table to just show users with that status
- **Timezone** – Select this option then, to filter the table to show users in one timezone, type the hours + or - from UTC for that timezone (i.e. +11)

The user's table contains the following information for each user:

- **Username/Email** – The user's email address, which is also the username they must enter to log in to the Service Portal
- **First Name** – The user's first (or given) name
- **Last Name** – The user's last (or family) name
- **Phone** – A contact telephone number for the user
- **Status** – Whether this user account is **Enabled** or **Disabled**. If a user account is listed as Disabled, the user will not be able to access the Service Portal.
- **Timezone** – Which timezone the user is normally based in
- **Last Login** – The last time and date when the user logged into the Service Portal
- **Role** – The user's role: **Tenant Administrator** or **Tenant User**
- **Tenant** – The name of the tenancy this user belongs to.
- ✎ – Edit the selected user
- 🗑 – Delete the selected user

Managing Users

From the user's table you can create new users and delete user accounts you no longer need. You can also edit user accounts to update details, change a user's role, or enable/disable their user account.

> **Caution:** If you delete all of your Tenant Administrator accounts you need to contact your provider to ask them to create a new one for you.

To create a new user

> **Note:** A password must be at least 8 characters long; including 1 number, 1 lowercase character, 1 uppercase character and 1 special character from the following list: $@#!%*?&^-_~.:(){}[]?.

1. From the main toolbar of the Service Portal, click **System**.
2. Click **Create User**.
3. Enter the following details for the new user:
    - **Email** – Type in the user's email address. This will also be their username.
    - **First Name** – Type in the user's first (or given) name.
    - **Last Name** – Type in the user's last (or family) name.
    - **Role** – Use the drop-down to select the user's role: Tenant Administrator or Tenant User.
    - **Status** – By default **Enabled** is selected. You can select **Disabled** to create a disabled user account which you can later choose to enable.
    - **Password** – Type a password for this user. They will be able to change this later.
    - **Confirm Password** – Re-type the password.
    - **Phone** – (Optional) Type in a contact telephone number for the user.
    - **Timezone** – From the drop-down, select the timezone this user is normally based in.
    - **Suppress Emails** – Select any of the check boxes to stop the user from receiving emails about specific alerts or reports.
4. Click **Save**.

> **Note:** You can edit ✎ or delete 🗑 users from the Users table.

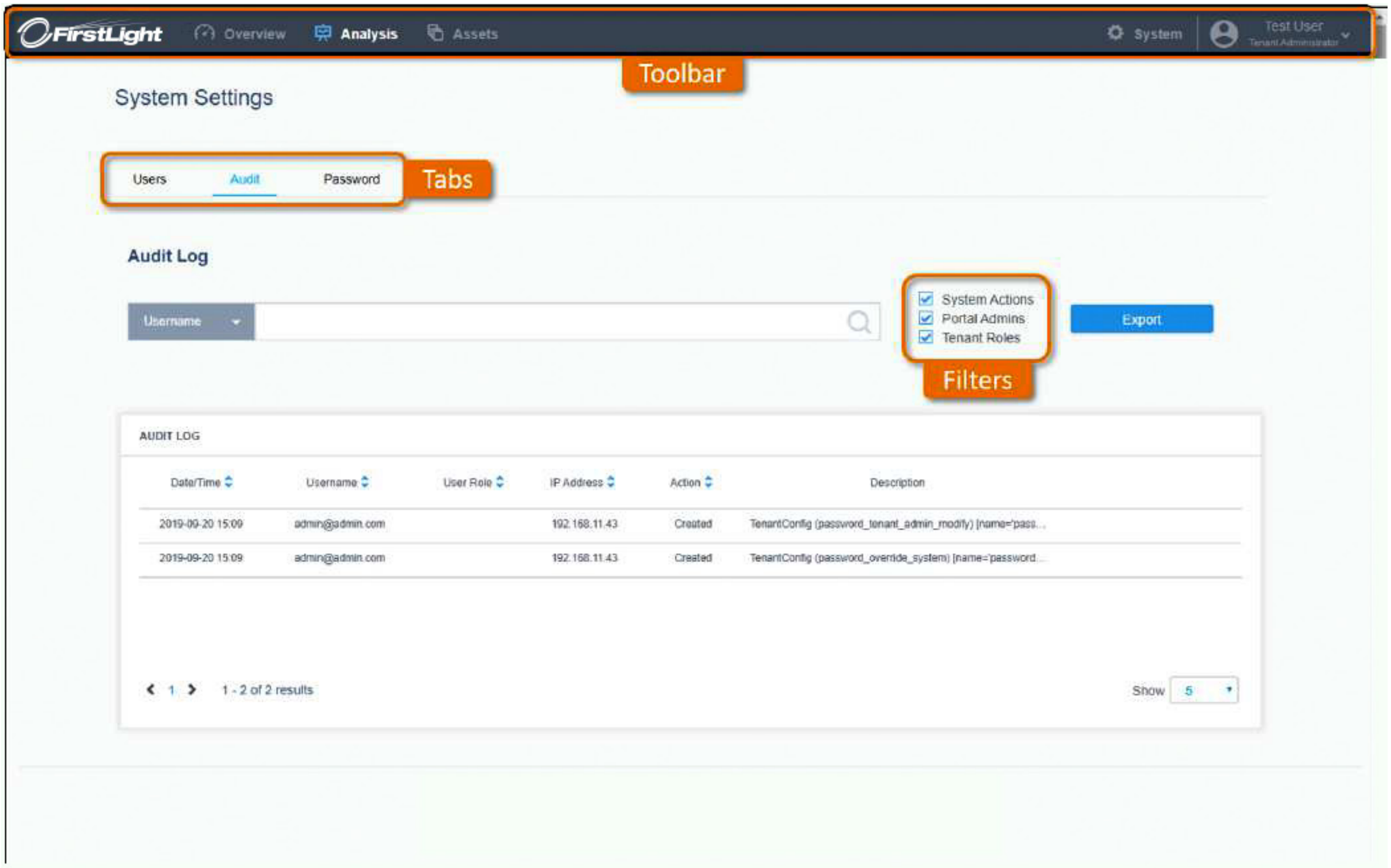
User Audit Log

To view user activity on your Service Portal you can use the audit log to see a list of every user action performed on the portal.

If you want to find out which user performed a task on a specific day you can filter the log by date/time. Or if you want to see everything a specific user has done you can search the log by username. You can combine these filters to see what a specific user was doing at a specific time.

Audit Settings Screen

You can navigate to the Audit tab of the System Settings Screen by clicking **System** on the main toolbar then the **Audit** tab.



AUDIT LOG

Date/Time	Username	User Role	IP Address	Action	Description
2019-09-20 15:09	admin@admin.com		192.168.11.43	Created	TenantConfig (password_tenant_admin_modify) [name='pass...
2019-09-20 15:09	admin@admin.com		192.168.11.43	Created	TenantConfig (password_override_system) [name='password...

The **Search** bar and drop-down at the top of the Audit tab enables you to search for specific actions. You can select one of the following categories and type a search term:

- **Username** – To find all actions performed by a user, select Username and type a search term to only display entries which contain the search term in the username field

- **User Role** – To find all actions by users with a specific user role (e.g. all actions performed by Tenant Administrators in the selected time period)
- **IP Address** – To find all actions performed from an IP address, select IP Address and type a search term to only display entries which contain the search term in the IP Address field
- **Action** – To find all instances of a specific action (e.g. Logged In)
- **Description** – To find all instances of a specific description term appearing in the audit log

Next to the search bar, you can use the checkboxes to filter your results:

- **System Actions** – Show or hide all actions performed by the System, rather than actions tied to a user (e.g. a server restart)
- **Portal Admins** – Show or hide all actions performed by Portal Administrators
- **Tenant Roles** – Show or hide all actions performed by Tenant Administrators and Tenant Users

You can use the **Timescale** filter drop-down to view actions from a specific time period:

- **Last Hour** – Only data from the last hour
- **24 Hours** – Only data from the last 24 hours
- **7 Days** – Only data from the last 7 days
- **30 Days** – Only data from the last 30 days
- **Custom** – You can use the date/time fields to set a start date and time in the first field then an end date and time in the second field. The table then shows only data from that time period.

Above the Audit log is the **Export** button, which you can use to download the current view of the audit log as a .csv file.

> **Note:** Any filters applied to the Audit log, at the moment you press Export, will affect the exported audit log. For example, if you set the timescale to 7 days and click Export, you will get a .csv file containing the last 7 days actions.

The audit log displays a list of the actions within the selected time period and, if you choose to, that were performed by the searched for user. It contains the following information for each action:

- **Date/Time** – When the action occurred
- **Username** – The user who performed the action
- **User Role** – The role of the user who performed this action
- **IP Address** – The IP address from which the user accessed the Service Portal
- **Action** – What action was performed
- **Description** – Further details of the action. If the description is truncated, hover over this field to see the full text.

Exporting the Audit Log

You can export the Audit Log as a .csv file. Any filters you apply to the Audit Log are used to filter the .csv file before it is created.

To export the Audit Log

1. From the main toolbar of the Service Portal, click **System**.
2. Open the **Audit** tab.
3. Apply any filters you require to the Audit Log.
4. Click **Export**.
5. A .csv file of the filtered Audit Log will now download in your browser.

Password Expiration Options

For security reasons, all users in the FirstLight Service Portal must reset their password after a period of time. You can configure how the Service Portal handles this process, using the password expiration options.

Password warning and grace periods

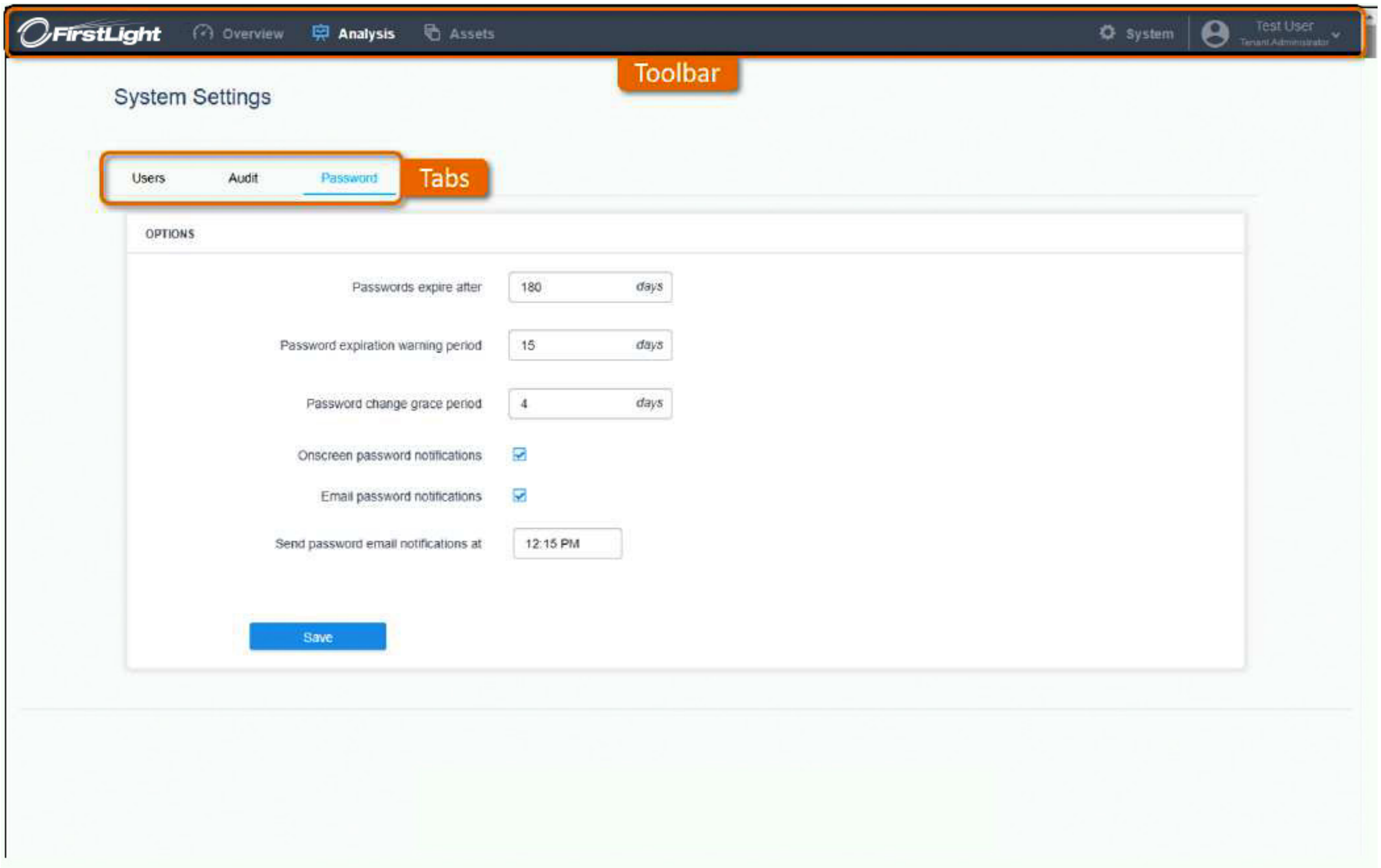
When a password expires, the user will no longer be able to log in to the Service Portal. To avoid this they need to change their password during the warning period or the grace period:

- **Warning Period** – During the warning period before the password expires, the user can change their password using the **Change Password** feature in the Account drop-down or the **Password Recovery** link on the log in screen. You can use notification emails and/or onscreen notifications to notify a user that they are in the warning period.
- **Grace Period** – During the grace period after the password expires, the user can still change their password using the **Password Recovery** link on the log in screen. They will not be notified they are in the grace period.

If a user does not change their password during the warning period or grace period, they must contact their administrator or FirstLight to have the password reset.

Password Settings Screen

You can navigate to the Password tab of the System Settings Screen by clicking **System** on the main toolbar, then the **Password** tab.



System Settings

OPTIONS

Passwords expire after: 180 days

Password expiration warning period: 15 days

Password change grace period: 4 days

Onscreen password notifications: ☑

Email password notifications: ☑

Send password email notifications at: 12:15 PM

You can set the following password options:

- **Passwords expire after** – The number of days after a password has been set when it needs to be reset. Once a password expires the user will not be able to log in to the Service Portal until they change the password.
- **Password expiration warning period** – The number of days before a password expires that the Service Portal starts creating notifications. During the warning period you can use the **Change Password** feature to set a new password.
- **Password change grace period** – The number of days after a password expires that the user can still use the **Password Recovery** link on the log in screen to reset the password. After that period, they must have an Administrator reset the password.
- **Onscreen password notifications** – Select the checkbox to enable onscreen password notifications when a user is logged in during the expiration warning period.
- **Email password notifications** – Select the checkbox to enable email password notifications. The email is sent once a day during the expiration warning period.
- **Send password email notifications at** – If you have enabled **Email password notifications**, this is the time of day that the Service Portal sends an email notification.

Managing Password Expiration Options

You can change the password expiration options for all users on your tenancy.

To edit the password expiration options

1. From the main toolbar of the Service Portal, click **System**, then the **Password** tab.
2. You can edit the following options:
   - **Passwords expire after** – (Default: 180 days) Type how many days before a user's password expires.
   - **Password expiration warning period** – (Default: 15 days) Type how many days before expiration the Service Portal should begin warning the user.
   - **Password change grace period** – (Default: 4 days) Type how many days after expiration the user will still be able to change their password themselves. If the user goes past this grace period, an Administrator will have to reset their password for them.
   - **Onscreen password notifications** – (Default: Enabled) Check the box to enable onscreen notifications of upcoming password expiration. Uncheck the box to stop these notifications from appearing.
   - **Email password notifications** – (Default: Enabled) Check the box to enable email notifications of upcoming password expiration being sent to the user's email address. Uncheck the box to stop these emails being sent.
   - **Send password email notifications at** – (Default: 12:15 PM) If you have enabled **Email password notifications**, you can choose the time those notification emails are sent to the user.
3. When you're happy with the settings, click **Save**.

   > **Tip:** If you don't want to save your changes, navigate away from the page. When you return to the Password tab, the options will have returned to their previous saved state.

Assets

An asset is an entity protected by the DDoS service, which is defined by one or more IP addresses (an asset can be anything from a single appliance to a whole network). When they created the FirstLight DDoS Service Portal account for your organization, FirstLight populated a list of your protected assets within their network. The attack traffic you see, in the System Overview and Attack Analysis screens, is defined by the destination IP addresses in your asset list.

The assets added to your asset list by your provider are called **Assigned Assets** and you can use the Asset View drop-down, on the Asset Screen, to view all of your Assigned Assets.

To enable you to track certain IP addresses or ranges, you can identify them as **Named Assets**. The name you give will appear in the charts, alerts, and reports whenever the IP address, or an address in the Named Asset range is attacked. For example, if you have multiple websites, you may want to associate the website names with each IP Address to enable you to quickly spot which website has been attacked. You can use the Asset View drop-down to view all of your Named Assets. Named Assets can be nested. For example, a tenant may wish to create a Named Asset for a specific location, and then also create Named Assets for each server within that location. You can use the Asset View drop-down to view all of a tenant's Named Assets.

FirstLight can also add and modify Named Assets.

> **Note:** Named assets cannot overlap one another. A nested Named Asset must be contained entirely by the Named Asset above it.

Asset Groups

You can organize assets into groups. Once you create a group, you can edit a Named Asset to assign it to a group. The Asset Groups tab then enables you to view all the IP addresses associated with each group. Alternatively, you can type the group name into the Search bar on the Assets tab to filter the table to only show assets in that group.

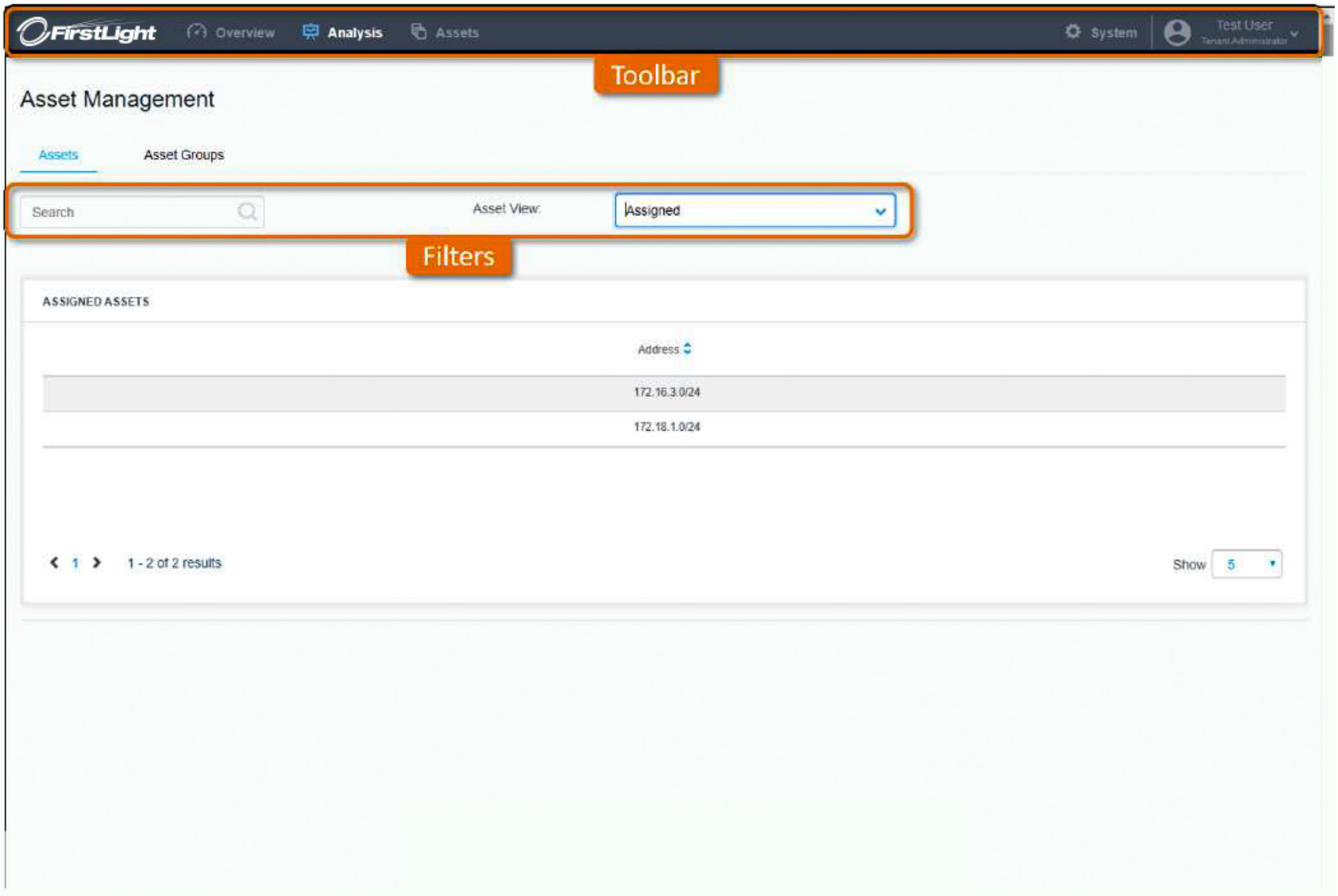
For example, you may have a few similar services you want to keep track of together. You could create a Named Asset for each service, and then add all of those Named Assets into an asset group. The asset group name will then appear with the Named Asset name on charts, reports and alerts when an IP address in that group is attacked.

FirstLight can also add and modify asset groups.

> **Tip:** You can also use the search bar in the Overview and Analysis screens to locate information about a Named Asset using the name or asset group.

Assets screen

You can navigate to the Assets tab by clicking **Assets** on the main toolbar then the **Assets** tab.



You can use the **Search** field to find a specific asset. As you type, the table will only display results that include the search term in one of its fields. You can use the **Asset View** drop-down to display assets in the table by:

- **Assigned** – All of the IP addresses assigned to this tenant
- **Named** – Only assets that you or the tenant have named

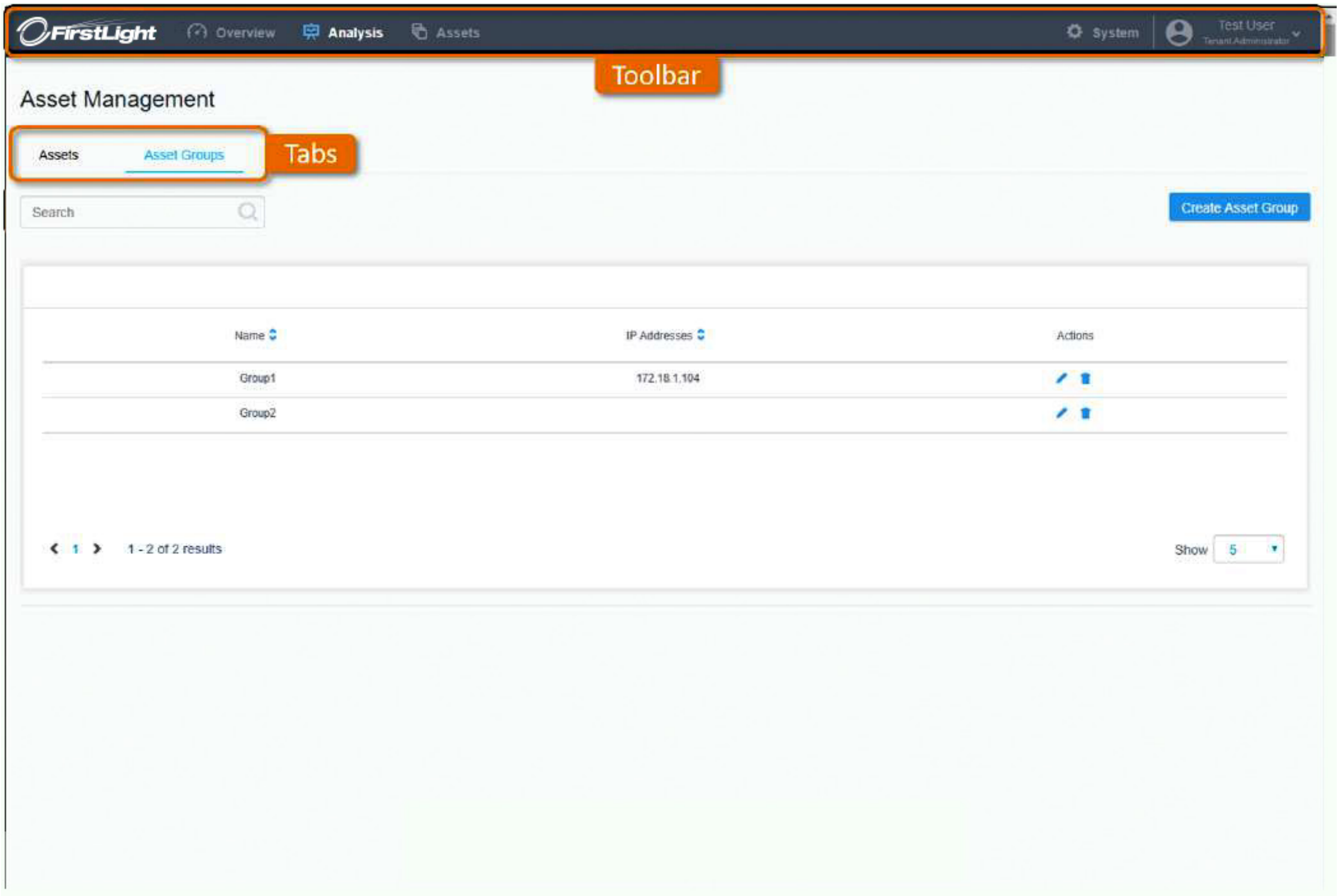
The assets table contains the following information for each asset:

- **Address** – The IP address or range of this asset
- **Asset Name** – (Named Assets view only) The name you have chosen for this asset. If this is not a Named Asset, this column is blank.
- **Asset Group** – (Named Assets view only) The group this asset belongs to. If you have not assigned it to a group, this column is blank.
- ✎ – (Named Assets view only) Edit the selected asset's name or assign this asset to a group

Note: When you view the asset list as an **Asset Summary**, you can add names to ranges and subsets. Those names are applied to all of the IP addresses contained in that range or subset. When you view the asset list as **All Assets**, you can give names to individual IP addresses. This overrides the range or subset names.

Asset Groups screen

You can navigate to the Asset Groups tab by clicking **Assets** on the main toolbar then the **Asset Groups** tab.



Asset Management

Name	IP Addresses	Actions
Group1	172.18.1.104	✎ 🗑
Group2		✎ 🗑

1 - 2 of 2 results

You can use the **Search** field to find a specific group. As you type, the table will only display results that include the search term in one of its fields. The asset groups table contains the following information for each group:

- **Name** – The name you have chosen for this asset group.
- **IP Address** – The IP addresses of the assets assigned to this group. If you have not assigned any assets to this group yet, this column is blank.
- ✎ – Edit the selected group's name
- 🗑 – Delete the selected group

Managing Assets

FirstLight populates the asset list with the IP addresses which are protected by the service. You can give these assets more familiar names and arrange them into convenient groups.

Prerequisites

If you want to add an asset to a group, you first need to create a group.

To add a Named Asset

1. From the main toolbar of the Service Portal, click **Assets**.
2. You should be on the **Assets** tab.
3. From the Asset View drop-down, select **Named**.
4. Click **Add Asset**.
5. Type in the IP **Address**, CIDR or range that you want to identify as a Named Asset. This must be all or part of a single Assigned Asset from the Assigned Asset list.
6. Type a **Name** for this Named Asset.
7. (Optional) Select an Asset **Group** from the drop-down.
8. Click **Save**.

> **Note:** You can edit ✏ or delete 🗑 Named Assets from the Named Assets table. Deleting the Named Asset doesn't affect the Assigned Asset, it only removes the name from the selected IP range.

To add an asset to a group or move an asset to a different group

1. From the main toolbar of the Service Portal, click **Assets**.
2. You should be on the **Assets** tab.
3. In the asset list, locate the asset you want to edit and click ✏ the edit button.
4. From the drop-down, select an **Asset Group**.
5. Click **Save**.

> **Note:** To remove an asset from a group, edit the asset then click the **x** in the top right of the asset group field.

Managing Asset Groups

To make it easier to view related assets together, you can create asset groups and assign all the related assets to that group. Then, if you want to look at all of your similar assets together in the attacks table or assets table, you can search for the asset group name.

To create a new asset group

1. From the main toolbar of the Service Portal, click **Assets**.
2. Click the **Asset Groups** tab.
3. Click **Create Asset Group**.
4. Type a name for your group and click **Save**.

> **Note:** You can edit ✏ or delete 🗑 groups from the Asset Groups table.

Service Overview and Attack Analysis

You can use the Service Overview and Attack Analysis screens of the FirstLight DDoS Service Portal to analyze DDoS attacks which are prevented from impacting your protected assets.

The Service Overview screen displays information on prevented attacks against all your protected assets.
You can change the timescale for this screen and, if your date range includes the current date and time, you can see ongoing attacks.

The Attack Analysis screen enables you to search more specifically for attacks, and filter those results by date range. For example, if you were looking for an attack that happened yesterday to an asset called Server1, you could select **Asset Name** from the drop-down list and then type "Server1" into the search field. Then, from the date filters, you could select **24 Hours**. The attack table would now show only attacks in the last 24 hours against an IP address that is associated with Server1.

Each attack has a unique Attack ID which you can use to identify it, when discussing with a provider. You can also expand each attack in the table, to see a chart of its traffic profile, where you can use the sliders to focus in on the blocked and allowed traffic for specific times during that attack.

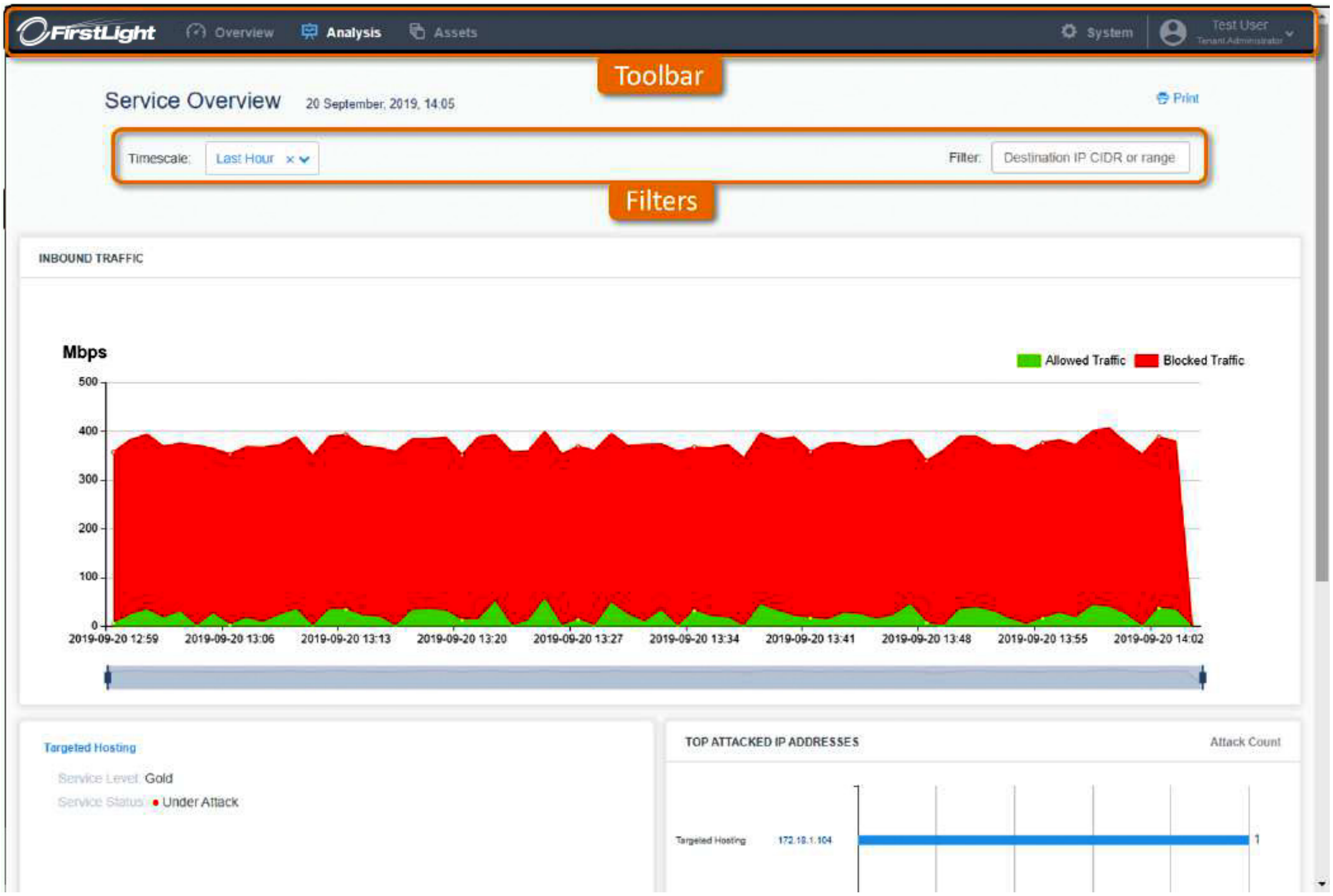
> Tip: You can click on a piece of information in a chart in the Overview screen, and the Attack Analysis screen will open showing the data point you clicked in the Overview chart.

Print attack reports

In the top right corner of the Service Overview and Attack Analysis screens there is the print button. This enables you to print a report from the information you are currently looking at. On the Service Overview screen this button prints the charts and attack table for the current date range you have selected. On the Attack Analysis screen this button prints the attacks table filtered by the Search terms and date filters you have selected.

Service Overview screen

You can navigate to the Service Overview screen by clicking **Overview** on the main toolbar.



Service Overview 20 September, 2019, 14:05

Timescale: Last Hour

Filter: Destination IP CIDR or range

Targeted Hosting

Service Level: Gold

Service Status: ● Under Attack

Targeted Hosting 172.18.1.104

Filters

The date filters at the top of the Service Overview screen change the charts and table below to show only data for that timescale. You can click **Timescale** to select from a list of date filters:

- **Last Hour** – Only data from the last hour
- **24 Hours** – Only data from the last 24 hours
- **7 Days** – Only data from the last 7 days
- **30 Days** – Only data from the last 30 days
- **Custom** – Use the date/time fields to set a start date and time in the first field then an end date and time in the second field. The charts and table below then show only data from that time period.

The Destination IP CIDR or range **Filter**, at the top right of the screen, can be used to show only the specified Destination IP (DIP), CIDR, or range on the charts.

The filters affects all charts and tables on the Service Overview screen:

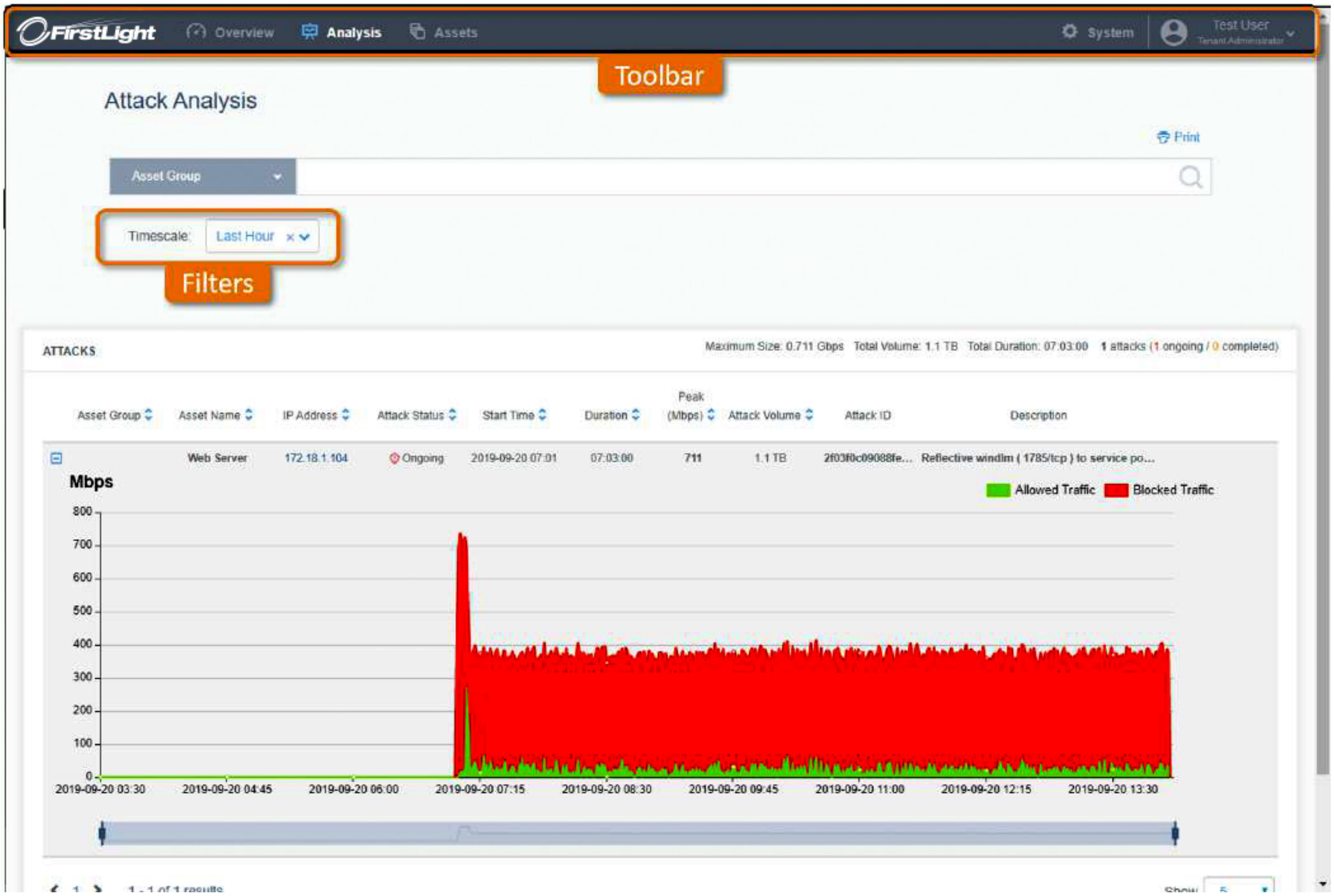
- **INBOUND TRAFFIC** chart – Displays the sampled allowed inbound traffic and sampled blocked traffic (in mega-bits per second) for your protected assets, over the selected time period.
  The green area on the chart denotes allowed traffic and the red area denotes blocked traffic. You can hover over the areas to see exact values of allowed or blocked traffic. You can also hide/show a type of traffic by clicking on **Allowed Traffic** or **Blocked Traffic** in the top right of the chart.
  To focus on a specific section of the time period you can use the sliders on the smaller line chart below the main display. Slide them in to focus on a particular time frame and slide them out to view the entire time period again.

- **TOP ATTACKED IP ADDRESSES** chart – Displays the 5 IP addresses that received the most attacks during the selected time period. The exact number of attacks is displayed at the end of each bar.
- **ATTACKS** table – Displays every attack on your assets during the selected time period. In the top right corner you can see the total number of attacks broken down into **ongoing** and **completed**.
  At the top of the Attacks table, you can view a summary of the current table content. This shows the **Maximum Size** of attacks, **Total Volume** of all attacks, **Total Duration** of the attack period shown in the table, and the number of **attacks** listed broken down into **ongoing** and **completed**.
  You can re-order the table using the column headers and refresh the table using ↻ the refresh icon.
  The Attacks table displays the following information for each attack:
  - **Asset Name** – If the IP address is part of a named asset this is displayed here. Otherwise this field is blank.
  - **IP Address** – The IP address which is the target of the attack. Click to view all attacks against this IP address.
  - **Attack Status** – An attack can be **Ongoing** or **Completed.**
  - **Start Time** – The time that the attack traffic was first detected.
  - **Duration** – For an ongoing attack, this is the amount of time since the attack started. For a completed attack, this is the total amount of time attack traffic was detected .
  - **Peak (Mbps)** – For an ongoing attack, this field shows the current peak value. For a completed attack it shows the highest rate of attack traffic detected during the attack in megabits per second (mbps).
  - **Attack Volume** – The volume of traffic sent over the duration of this attack. Only available for SWA 9.7.0 and later, other versions show **n/a**.
  - **Description** – A summary of the attack characteristics. If the description is truncated, hover over it to see the full text.

You can click 🖶 Print in the top right to print the selected view or save it in PDF format.

Attack Analysis screen

You can navigate to the Attack Analysis screen by clicking **Analysis** on the main toolbar.



ATTACKS

Maximum Size: 0.711 Gbps Total Volume: 1.1 TB Total Duration: 07:03:00 1 attacks (1 ongoing / 0 completed)

Asset Group	Asset Name	IP Address	Attack Status	Start Time	Duration	Peak (Mbps)	Attack Volume	Attack ID	Description
	Web Server	172.18.1.104	Ongoing	2019-09-20 07:01	07:03:00	711	1.1 TB	2f03f0c09088fe...	Reflective windim (1785/tcp) to service po...

The **Search** bar and drop-down at the top of the Attack Analysis screen enables you to search for specific attacks. You can select one of the following categories and type a search term:

- **Attack ID** – If you type a full Attack ID, the Attacks table only shows attacks made against that Attack ID. If you type a partial Attack ID, the Attacks table shows all results that include the search term in the Attack ID field.
- **Asset Name** – The Attacks table only shows results that include the search term in the Asset Name field.
- **Asset Group** – The Attacks table only shows results that include the search term in the name of the Asset Group.

Just like the Service Overview screen you can also use the date filters to change the time period for which the table shows data. You can use the filter and search individually or together to narrow down the results in the Attacks table.

Common Analysis Tasks

On the Service Overview and Attack Analysis screens of the FirstLight DDoS Service Portal, you can use the date and search filters to view specific attack data. You can use these tools individually or together to filter the tables and charts to only show the information you need. The following are some of the most common tasks you may want to complete using these tools:

To view any ongoing attacks against your assets

1. From the main toolbar of the Service Portal, click **Overview**.
2. At the **Timescale** drop-down, select **Custom**.
3. Make sure that the second field is showing the current date.
4. Look at the **ATTACKS** table. Click the **Attack Status** column header to reorder the table so that all ongoing attacks are at the top.

To view the most attacked IP addresses in the past week

1. From the main toolbar of the Service Portal, click **Overview**.
2. From the **Timescale** drop-down select **7 Days**.
3. Look at the **TOP ATTACKED IP ADDRESSES** chart. Here you can see a visualization of the top 5 most attacked IP addresses in your network. You can see the exact number of attacks each experienced at the end of the blue bar. To the left, you can see the tenant associated with this IP address.

To view all attacks against a single asset

1. From the main toolbar of the Service Portal, click **Analysis**.
2. From the Search drop-down, select **Asset Name**.
3. In the search bar, type the name of the asset whose attacks you want to view.
4. The **ATTACKS** table now shows only the attacks which have that search term in the Asset name column.

To view all attacks between two dates

1. From the main toolbar of the Service Portal, click **Analysis**.
2. At the **Timescale** drop-down, select **Custom**.
3. Click into the first date field. Use the calendar to select the first date. If you want to set a time, click the time at the bottom (e.g. 00:00) and use the arrows to set the hours and minutes. To return to the calendar, click the date at the top (e.g. 01/01/2019).
4. Click into the second date field and repeat the process for the closing date.
5. The **ATTACKS** table now shows only the attacks which have happened between your two selected dates.

To view all attacks against an asset in the past day

1. From the main toolbar of the Service Portal, click **Analysis**.
2. From the Search drop-down, select **Asset Name**.
3. In the search bar, type the name of the asset whose attacks you want to view.
4. From the **Timescale** drop-down select **24 Hours**.
5. The **ATTACKS** table now shows only the attacks which have happened in the last 24 hours and that contain that search term in the Asset name column.

To print a report showing all attacks against an IP address in the last week

1. From the main toolbar of the Service Portal, click **Analysis**.
2. From the Search drop-down, select **IP Address**.
3. In the search bar, type the IP address you want to view attacks against.
4. From the **Timescale** drop-down select **7 Days**.
5. The **ATTACKS** table now shows only the attacks which have been directed at that IP address over the last week.
6. Click Print. Adjust any printer settings you require, then click Print.
7. You will print a report listing all the attacks directed at that IP address over the last week.

Contacting FirstLight Customer Support

For problems with the DDoS portal, Contact Customer Repair at

Repair@FirstLight.net or call 888-832-4976

during the hours of 8 a.m. to 5 p.m. Monday through Friday.