



# Corero Network Security

## **SmartWall Service Portal Admin Guide**

Software Version 2.1.0

12 July 2023

Part Number: 9302-0210-01-J

## Legal and Copyright Information

Corero Network Security, Inc. (Corero) reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of Corero to provide notification of such revision or change. Corero provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. Corero may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If you are a United States government agency, this documentation and the software described herein are provided to you subject to the following:

This paragraph applies to all acquisitions of the software by or for the United States Government, or by any prime contractor or subcontractor (at any tier) under any contract, grant, cooperative agreement or other activity with the United States Government (collectively, the “Government”). All technical data and computer software are commercial in nature and developed solely at private expense. The software and documentation respectively are “commercial computer software” and “commercial computer software documentation” as defined in DFARS 252.227-7014 (June 1995) and “commercial items” as defined in FAR 2.101 (a) and, to the maximum extent permitted by law, are provided with only such rights as are provided in Corero’s standard commercial license for the software and documentation and this notice. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (November 1995) or FAR 52.227-14 (June 1987), whichever is applicable. Corero’s standard commercial license for the software and documentation and this notice shall govern the Government’s use of the software, documentation, and technical data, and shall supersede any conflicting contractual terms or conditions. If these terms and conditions fail to meet the Government’s needs or is inconsistent in any respect with Federal law, the Government must return the software and the documentation unused to Corero. The following additional statement applies only to acquisitions governed by DFARS Subpart 227.4 (October 1988): “Restricted Rights – Use, duplication and disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT. 1988).” The Contractor is Corero Network Security, Inc.

You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this document.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Corero.

The products described in this document are protected by US Patent No. 9,442,782, US Patent No. 10,341,364, and European Patent No. 1319296.

Any software on removable media described in this documentation, is furnished under a license agreement which is located on the Corero web site.

Corero®, First Line of Defense®, SecureWatch®, and SmartWall® are registered trademarks of Corero Network Security, Inc. All other trademarks and registered trademarks are the property of their respective holders.

For warranty, licensing and maintenance agreement information, visit [http://www.corero.com/support/End\\_User\\_Agreements.html](http://www.corero.com/support/End_User_Agreements.html).

Copyright © 2014- 2023, Corero Network Security, Inc.

# CONTENTS

---

<b>Legal and Copyright Information</b>	<b>2</b>
<b>Contents</b>	<b>3</b>
<b>SmartWall Service Portal</b>	<b>9</b>
<b>Corero Concepts</b>	<b>10</b>
SmartWall System	10
Sample-based traffic information	11
Tenants	11
Assets	11
<b>Working in the Service Portal</b>	<b>11</b>
<b>Getting Started</b>	<b>13</b>
<b>System Requirements for Installation</b>	<b>14</b>
Minimum system requirements	14
Recommended system requirements	14
<b>Installing the Service Portal</b>	<b>15</b>
<b>Integrating the Service Portal into SmartWall</b>	<b>16</b>
Integrating the Service Portal with the SWA	16
Integrating the Service Portal with the CMS	17
Combined SmartWall TDD and TDS Service Portal Feeds	18
<b>Logging In to the Service Portal</b>	<b>20</b>
To log in to the Service Portal with a username and password	20
To log in to the Service Portal with a password token	20
To log in to the Service Portal with Single Sign-On	20
To log out of the Service Portal	20

# CONTENTS

---

<b>Tuning your Sample Rate</b>	<b>21</b>
<b>Changing your own Password</b>	<b>22</b>
To change your password from inside the Service Portal	22
To recover your password using email verification	22
<b>Editing your own User Profile</b>	<b>23</b>
To edit your user profile	23
<b>Configure the Service Portal</b>	<b>24</b>
<b>Authentication</b>	<b>25</b>
LDAP Authentication	25
Users Settings Screen	26
LDAP Settings Screen	28
Managing Users	31
Configuring LDAP Integration for Authentication Users	34
Configuring Single Sign-On	36
Password Settings	40
User Audit Log	46
Managing REST API Tokens	50
<b>Policy and Reporting</b>	<b>52</b>
Service Policy and Alerting	52
Scheduled Reporting	61
Usage Statistics	65
Remote Mitigation	67
Notification Settings	70
<b>Portal Management</b>	<b>73</b>
Licensing	73

---

# CONTENTS

Theme .....	76
Email Settings .....	81
HTTPS .....	85
Portal Health Monitoring .....	87
Diagnostics .....	90
Snapshots .....	95
Software Upgrade .....	98
System Actions .....	100
Custom Tenant Fields .....	102
<b>Tenants Overview .....</b>	<b>105</b>
<b>Tenant traffic and attacks .....</b>	<b>105</b>
<b>Assets .....</b>	<b>106</b>
Reassigning an Asset .....	107
<b>Tenant user roles .....</b>	<b>107</b>
<b>Tenant Management screen .....</b>	<b>107</b>
Create a tenant .....	108
Find a tenant .....	108
Navigate a tenant's options .....	109
<b>Creating a New Tenant .....</b>	<b>111</b>
Prerequisites .....	111
To create a new tenant .....	111
Next Steps .....	111
<b>Importing Multiple Tenants .....</b>	<b>112</b>
To import multiple Tenants .....	112
Next steps .....	113

# CONTENTS

---

<b>Managing a Tenant's Users</b>	<b>114</b>
To add a new user	114
<b>Managing a Tenant's Assets</b>	<b>115</b>
To add a new Assigned Asset	115
To add a new Named Asset	115
To create an asset group	116
<b>Importing Multiple Assets</b>	<b>117</b>
Prerequisites	117
To import multiple assets	117
<b>Viewing Tenant Attacks</b>	<b>119</b>
Prerequisites	119
To view a tenant's dashboard	119
<b>Viewing Tenant Audit Log</b>	<b>120</b>
To view a tenant's Audit Log	120
To export a tenant's Audit Log	121
<b>Managing Tenant-specific Notifications</b>	<b>122</b>
<b>Changing Tenant Details</b>	<b>123</b>
Accessing the Details tab	123
<b>Deleting a Tenant</b>	<b>124</b>
To delete an existing tenant	124
<b>Service Overview and Attack Analysis</b>	<b>125</b>
<b>Traffic charts</b>	<b>125</b>
Traffic considerations for Service Portals connected to a SmartWall	
TDD system	126

# CONTENTS

---

Differences between the Service Portal and SmartWall TDD attack charts .....	127
<b>Print attack reports .....</b>	<b>127</b>
<b>Service Overview screen .....</b>	<b>128</b>
Filters .....	128
Charts and tables .....	129
<b>Attack Analysis screen .....</b>	<b>132</b>
Filters .....	132
Charts and tables .....	133
<b>Common Analysis Tasks .....</b>	<b>136</b>
To view any ongoing attacks in your network .....	136
To view the tenants who experience the most attacks today .....	136
To view the most attacked IP addresses in the past week .....	136
To view all attacks against a single tenant .....	136
To view all attacks between two dates .....	137
To view all attacks against a tenant in the past day .....	137
To print a report showing all attacks against an IP address in the last week .....	137
<b>Service Portal REST API Overview .....</b>	<b>138</b>
<b>Accessing the REST API documentation .....</b>	<b>138</b>
Using the Swagger web interface .....	138
<b>Using the REST API .....</b>	<b>139</b>
Available operations .....	139
HTTP return codes .....	140
Versions .....	141

# CONTENTS

---

Etags .....	141
Using cURL .....	142
<b>Troubleshooting .....</b>	<b>144</b>
<b>Contacting Corero Customer Support .....</b>	<b>145</b>
Commenting on This Help Set .....	145
<b>Requesting Technical Support .....</b>	<b>146</b>
Self-Help Online Tools and Resources .....	146
Creating a Service Request with JTAC .....	146
<b>Requesting Licenses .....</b>	<b>147</b>

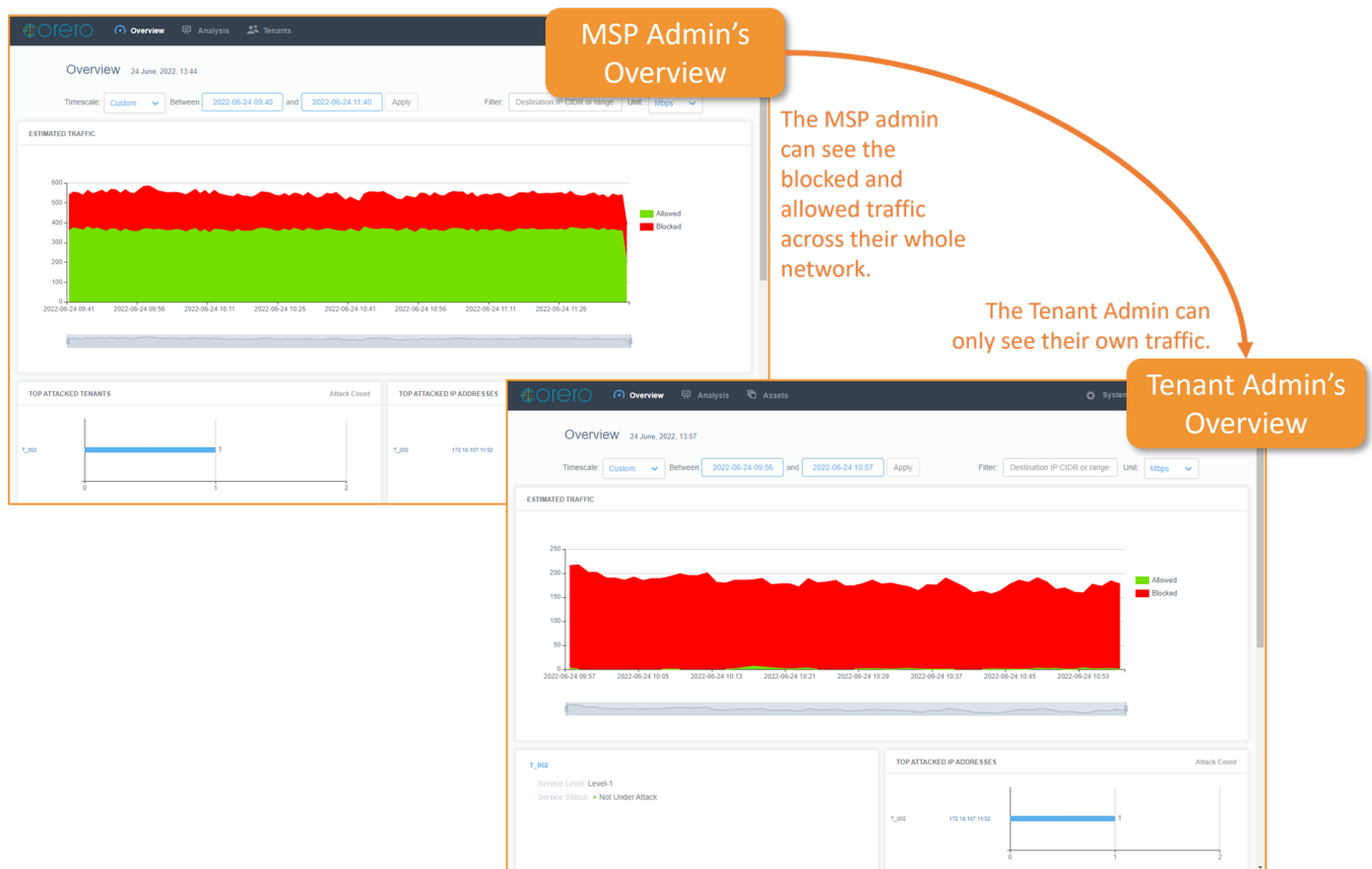


## SmartWall Service Portal

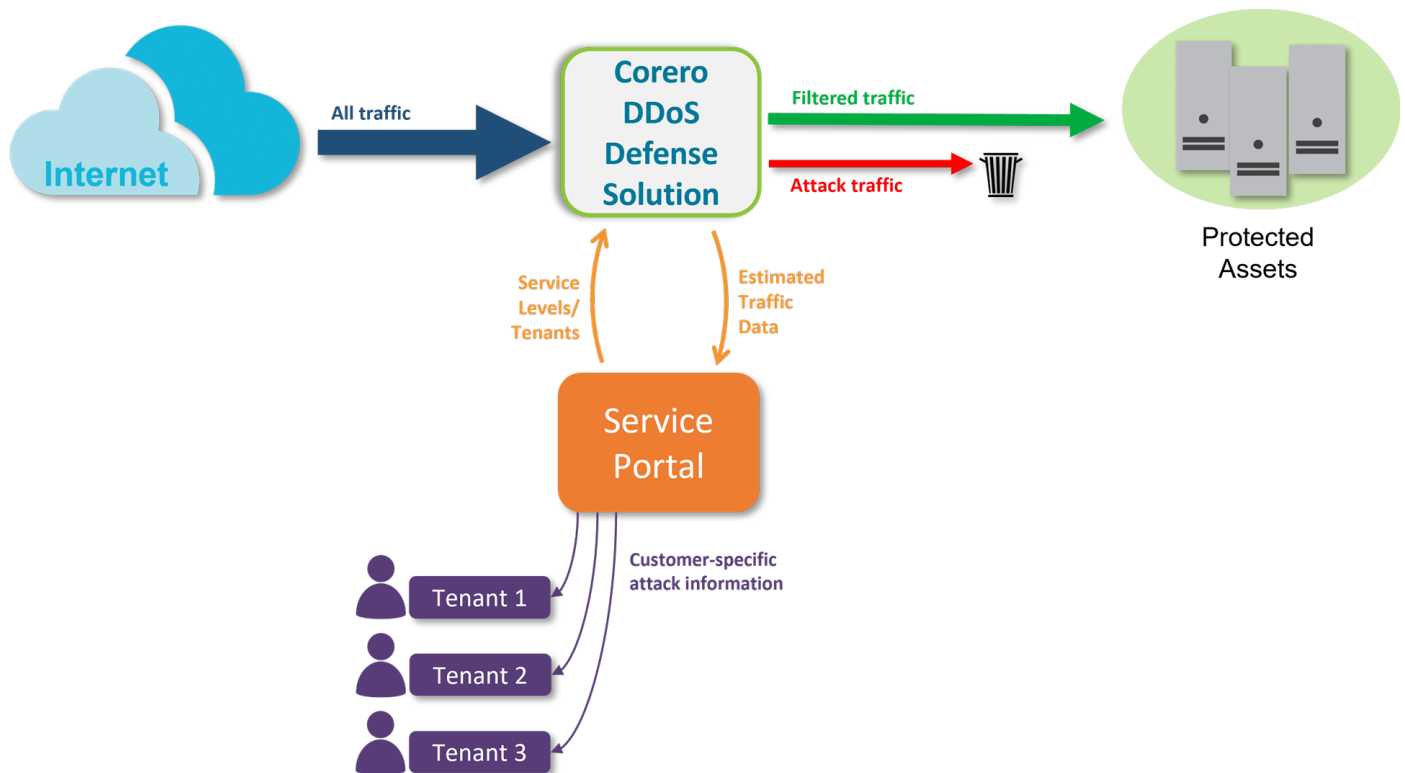
The SmartWall Service Portal enables you to offer Corero SmartWall DDoS Protection, as a managed service, to your customers.

The Service Portal uses sampled traffic data from your SmartWall Threat Defense System (SmartWall TDS) or SmartWall Threat Defense Director (SmartWall TDD). It displays the information in easy to read charts and reports. You can create reports for your customers to highlight the value they receive from the DDoS protection service, based on the number and size of the attacks you are protecting them from.

As the provider, you can view aggregate traffic data and analyze attacks across the whole network, which is protected by the SmartWall System, as well as viewing traffic data on a per-customer basis. Additionally, your customers are able to log into their own view of the Service Portal and see only the attack information that relates to their assets which you protect. This enables them to immediately see the benefit of the DDoS protection service both historically, and in real time. In the image below, a single customer is being attacked and the attack is being mitigated by the SmartWall System. The MSP Administrator and the customer can both see and analyze the attack.



## Corero Concepts



## SmartWall System

The Service Portal is used together with a Corero SmartWall System - either a SmartWall Threat Defense System (SmartWall TDS) or a SmartWall Threat Defense Director (SmartWall TDD). Both systems protect you from DDoS attacks by filtering out attack traffic before it can impact your network. Each SmartWall System is comprised of 3 main parts:

- Defense devices – In SmartWall TDS deployments they are used inline to mitigate DDoS attacks and, in SmartWall TDD deployments, they are used as detection engines to inform the edge routers what is attack traffic and should be blocked.
- SmartWall Central Management Server (CMS) – The management application which manages all the Defense devices and collates traffic samples for traffic analytics.
- SmartWall SecureWatch Analytics (SWA) – The analytics application where you can view realtime and historic traffic data. This application forwards sample traffic information from the CMS to the Service Portal to provide the traffic data for the Service Portal.

## Sample-based traffic information

Your SmartWall System (SmartWall TDD or TDS) sends metadata about traffic samples to the Service Portal to populate the inbound traffic charts and enable you to see what has been blocked or allowed by the SmartWall System. The traffic data you see in the Service Portal is generated from only the traffic samples it receives information about. Network overview information and attack-time data is always very accurate due to the high volume of samples. Peace-time data and DIP-specific information can be a less accurate estimate if the sample rate isn't high enough. You can configure how often these samples are sent to the Service Portal as needed.

## Tenants

You can add your customers to the Service Portal as tenants. Once you specify which IP addresses you have provisioned your tenant with, you can see DDoS attack information on a per-customer basis. You can also provide a tenant-specific version of the portal for each tenant, where they log in and view their own traffic information and receive reports on their mitigated DDoS attacks. A Tenant Administrator, or Tenant User, on the Service Portal can only view their own traffic data.

## Assets

An asset is an entity protected by your SmartWall System, which is defined by one or more IP addresses (an asset can be anything from a single appliance to a whole network). For each tenant, you need to specify which assets in your protected network belong to them. Assets can be named and grouped for improved recognition in reports and alerts.

## Working in the Service Portal

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

- **Chrome:** 97 or newer
- **Edge:** 97 or newer
- **Firefox:** 96 or newer
- **Safari:** 15 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 [Tenants](#) and [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

**Note:** Installing the Service Portal must be completed before you can use the system. If your Service Portal is already installed and running, skip to [Logging In to the Service Portal](#).

You can install the Service Portal using an OVA file (for ESXi systems) or a ZIP file (for KVM systems) provided by your Corero representative. Some of the code in the prerequisites and installation instructions can be copy and pasted once you declare values for the variables.

**Caution:** Sometimes copying text directly from a PDF also copies line breaks. If a copied command does not run, try copying it first into a plain text editor, to see if there are any unexpected characters or breaks.

Once you complete the installation process, you need to configure your SmartWall SecureWatch Analytics application to forward traffic information to the Service Portal.

At this point, you are ready to access the Service Portal through your browser and begin [configuring the portal to your requirements](#) and, ultimately, to on-board your [tenants](#).

## System Requirements for Installation

The SmartWall Service Portal must be installed on one of the following servers:

- Linux server (Redhat Enterprise 7, Centos 7, Ubuntu 16.04, Debian 9.9) using Kernel-based Virtual Machines (KVM).
- vCenter Server 6.5 or later with ESX/ESXi 6.5 or later.

Your specific hardware requirements depend on the amount of tenants you plan to on-board and the number of attacks your network normally experiences.

**Caution:** Keep the SmartWall Service Portal application and the underlying Linux operating system running the latest software to ensure you have the latest security patches. Please see [Software Upgrade](#) for full details.

### Minimum system requirements

The following requirements are necessary for a functional Service Portal:

- 4 vCores
- 16GB RAM
- 400 GB storage (SSD or SATA)

### Recommended system requirements

The following requirement are recommended for an application expecting multiple tenants and daily attacks:

- 8 vCores
- 32GB RAM
- 1TB storage (SSD or SATA)

**Note:** The data retention period for the Service Portal is 400 days. This ensures roughly 13 months of historical traffic data. If you need to modify the data retention period, please contact your support representative.

**Caution:** For TDD deployments, the Service Portal host must use an NTP time server the same as the other TDD applications. Differences in time between applications can cause unexpected behavior. See your operating system guide for instructions on configuring your host's time settings. By default, the Service Portal is installed with NTP enabled.

**Caution:** You may need to increase these requirements if you experience a large number of attacks, or you plan to onboard a large number of tenants.

## Installing the Service Portal

You are using an online-abridged copy of this user guide. For information on installing the SmartWall Service Portal, [contact your support representative](#) for a copy of the full **Corero SmartWall Service Portal User Guide**.

## Integrating the Service Portal into SmartWall

To fully integrate the SmartWall Service Portal into your SmartWall deployment, you need to connect it to the SWA and CMS applications. Connecting these applications enables the following functionality:

- Enabling the Service Portal feed allows the SWA to forward network traffic and attack data to the Service Portal
- Enabling SWA synchronization allows the SWA to configure rule actions based on Service Level data
- Enabling CMS synchronization is critical to attack reporting scoped by asset and tenant, as well as enabling the creation and updating of DAGs (Dynamic Address Groups) for tenant assets.

**Caution:** Enabling CMS synchronization is mandatory for correct operation of the Service Portal.

## Integrating the Service Portal with the SWA

**Note:** If you use a SmartWall Management Controller to host your SWA application, you can contact your Corero Support representative to have the SWA connected to your Service Portal.

### Prerequisites

You must be running CMS/SWA version 11.4.x/11.5.x or later.

### To enable the Service Portal Feed in the SWA

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **System > Settings > Service Portal Integration**.
3. To connect the SWA to a Service Portal and deliver the traffic and attack feed:
  - a. Under **Enable Service Portal Feed**, click the grey slider. It will turn green to show the connection is enabled.
  - b. Type in the **IP Address** of your Service Portal. If not using the default UDP port (5410) use format `<address>:<port>`.
4. (Optional) Unless you're combining SmartWall TDD and TDS Service Portal feeds, leave the **Report allowed traffic data** set to enabled.
5. (Optional) By default, **Report blocked traffic data only if destination is under attack** is enabled by default. Very small amounts of attack traffic may be blocked without creating an attack record, this setting stops those small blocked attacks appearing on Service Portal traffic charts. This feature can be disabled if you prefer to show those small attacks.
6. Click **Save**.



## **To enable Service Portal synchronization in the SWA**

To synchronize Service Level data between the Service Portal and the SWA, refer to the "Connecting a Service Portal to the SWA" topic in the Corero SmartWall TDD User Guide.

## **Integrating the Service Portal with the CMS**

### **Prerequisites**

- You must be running CMS/SWA version 11.4.x11.5.x or later.
- Your CMS must either be configured through the Service Portal Configuration service (in 11.8.x or later), or an installed Tenant Awareness Smart-Plugin (on earlier versions only).

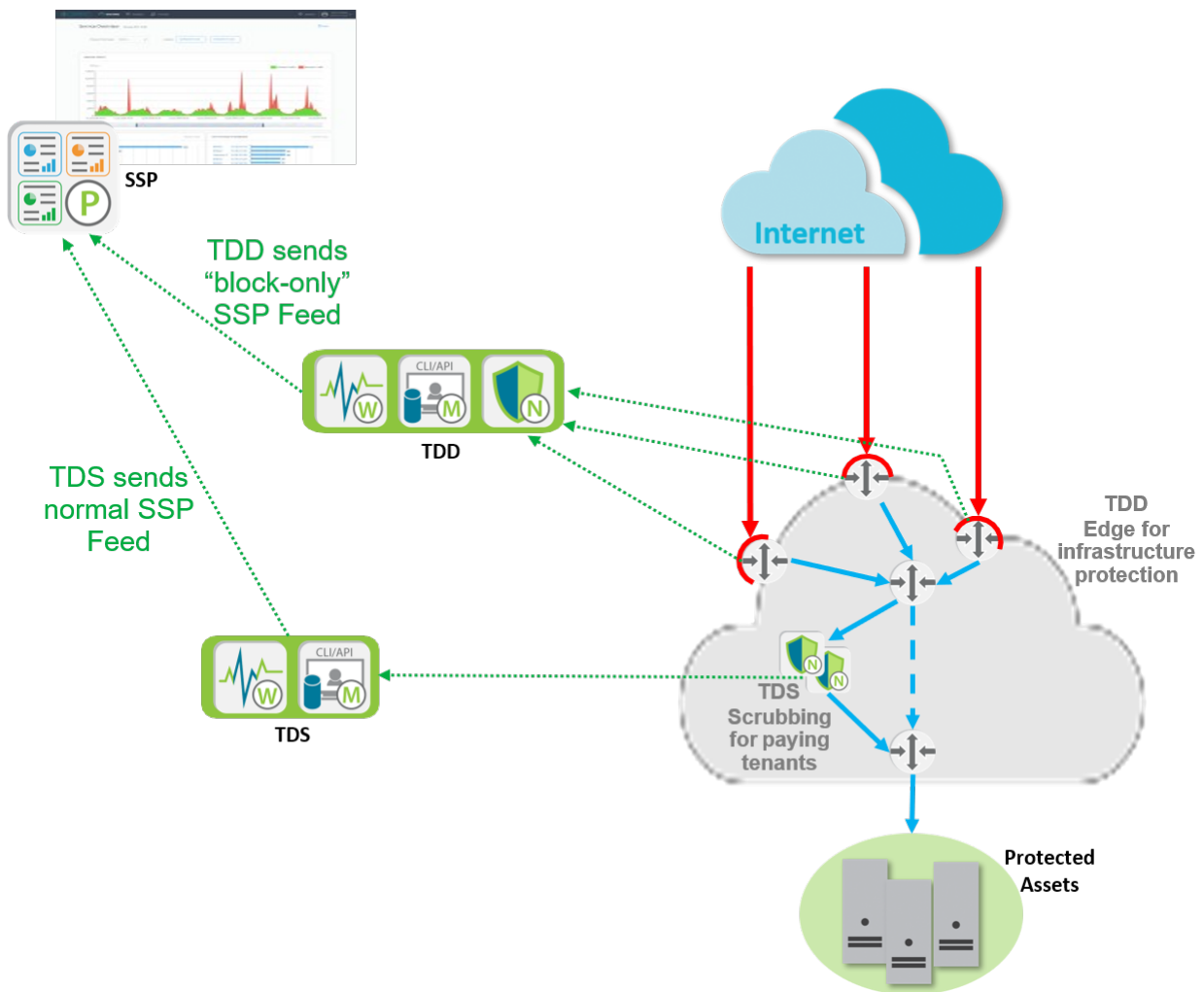
For details on configuring services in the CMS, you should consult the Corero SmartWall CMS User Guide for information specific to your software version. For details on the installation and configuration of the Tenant Awareness Smart-Plugin, refer to the documentation supplied with that product.

## Combined SmartWall TDD and TDS Service Portal Feeds

SmartWall TDD delivers large scale DDoS protection at the edge of your network, and can be combined with SmartWall TDS for more fine-grained and sophisticated DDoS protection. For example, this may be to provide a DDoS service where paying tenants can gain additional protection from SmartWall TDS, enhancing the SmartWall TDD protection provided for all.

When deployed in this way, both the SmartWall TDS and TDD systems may deliver traffic statistics to the SmartWall Service Portal. This could lead to traffic being counted more than once in the Service Portal.

To prevent this, you need to stop the SmartWall TDD from sending allowed traffic information. The SmartWall TDD will then only forward information on the traffic it blocks. This leaves the SmartWall TDS system to report on the traffic it blocks and traffic which has been allowed through both the SmartWall TDD and TDS systems to the internal network.



## To enable/disable sending allowed traffic information to a Service Portal

1. In a browser open the SWA UI.
2. Navigate to **System > Settings > Service Portal Integration**.
3. Ensure your [Service Portal connection](#) is correctly configured.
4. Use the **Report allowed traffic data** slider to enable or disable this feature as required:
  - It should be disabled on the SmartWall TDD in a combined SmartWall TDD and TDS environment.
  - It should be enabled on:
    - A SmartWall TDD only environment
    - A SmartWall TDS only environment
    - The SmartWall TDS in a combined SmartWall TDD and TDS environment
5. Click **Save**.

## Logging In to the Service Portal

The login page appears the same for SmartWall Service Portal providers and tenants. You can [customize it to display your organization's logo and branding](#).

**Caution:** You are only allowed three failed login attempts before you must [reset your password](#).

### To log in to the Service Portal with a username and password

1. You will receive your login credentials from a Service Portal administrator.
2. In a browser, navigate to the web address for your Service Portal. This was created during the installation process.
3. Type in your **Username** and **Password**.
4. Click **Log in**.
5. The Service Portal opens on the Service Overview screen.

### To log in to the Service Portal with a password token

1. You will receive a password token via email. Copy the token to your clipboard.
2. In a browser, navigate to the web address for your Service Portal. This was created during the installation process.
3. Click **Apply Password Token**.
4. Paste the password token into the **Token** field.
5. Click **Apply**.
6. Type a **Password** and **Confirm Password**.
7. Click **Save**.
8. The Service Portal opens on the Service Overview screen.

### To log in to the Service Portal with Single Sign-On

1. In a browser, navigate to the web address for your Service Portal. This was created during the installation process.
2. Click **Log in with Single Sign-On**.
3. On the displayed page, log in using the account credentials you use to sign in to your organization's other applications and systems.
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**.

## Tuning your Sample Rate

You are using an online-abridged copy of this user guide . For information on tuning your sample rate for the SmartWall Service Portal, [contact your support representative](#) for a copy of the full **Corero SmartWall Service Portal User Guide**.

## Changing your own Password

When you first access the SmartWall 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. MSP Administrators can [edit password settings](#).

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 user's 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 [alert emails](#) by checking the boxes next to any of the following:
  - **Service level status alerts**
  - **Attack status alerts**
  - **Remote mitigation alerts**
5. You can choose to suppress [report emails](#) by checking the boxes next to any of the following:
  - **Service overview reports**
  - **Per tenant reports**

**Note:** You cannot suppress Slack/ Teams alerts as these go to a designated channel, not to an individual.

6. 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 an MSP Administrator. If you are an MSP User, you can only [view policy information](#); you can skip to [Tenants](#) or [Service Overview and Attack Analysis](#) section of this guide.

When you first log in to your SmartWall Service Portal, there are a few tasks you need to perform before you begin onboarding tenants:

- [Adding your organization's logo to the Service Portal](#)
- [Setting up service levels](#)
- [Creating user accounts for other members of your organization](#)

As well as MSP Administrators, you can create MSP User accounts who can view attacks information and manage tenants, but not make any system changes.

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



## Authentication

Users can access the SmartWall Service Portal using their individual account credentials. When you first install the Service Portal there will only be one user account; the Service Portal administrator account you created during the installation process. MSP Administrators can create additional user accounts and, once you have Tenant Administrators, they can create users within their tenancy.

**Note:** The Service Portal can have a maximum of 12,000 users.

There are two user roles for the provider portal:

- **MSP Administrator** – Can view traffic data, analyze attacks, manage tenants, manage other MSP users, edit Service Portal system settings
- **MSP User** – Can view traffic data, analyze attacks and manage tenants

In tenant portals, there are two tenancy specific user roles:

- **Tenant Administrator** – Within their tenancy they can view traffic data, analyze attacks, manage assets, and manage other Tenant Administrators and Tenant Users
- **Tenant User** – Within their tenancy they can view traffic data, analyze attacks and view the asset list

Tenant Administrators and Tenant Users can only view attack data for the IP addresses in their tenancy's asset list and can only affect settings for their own tenancy within the Service Portal. You can [create Tenant Administrators and Users](#) in the Tenants screen or at the User screen (System>Users).

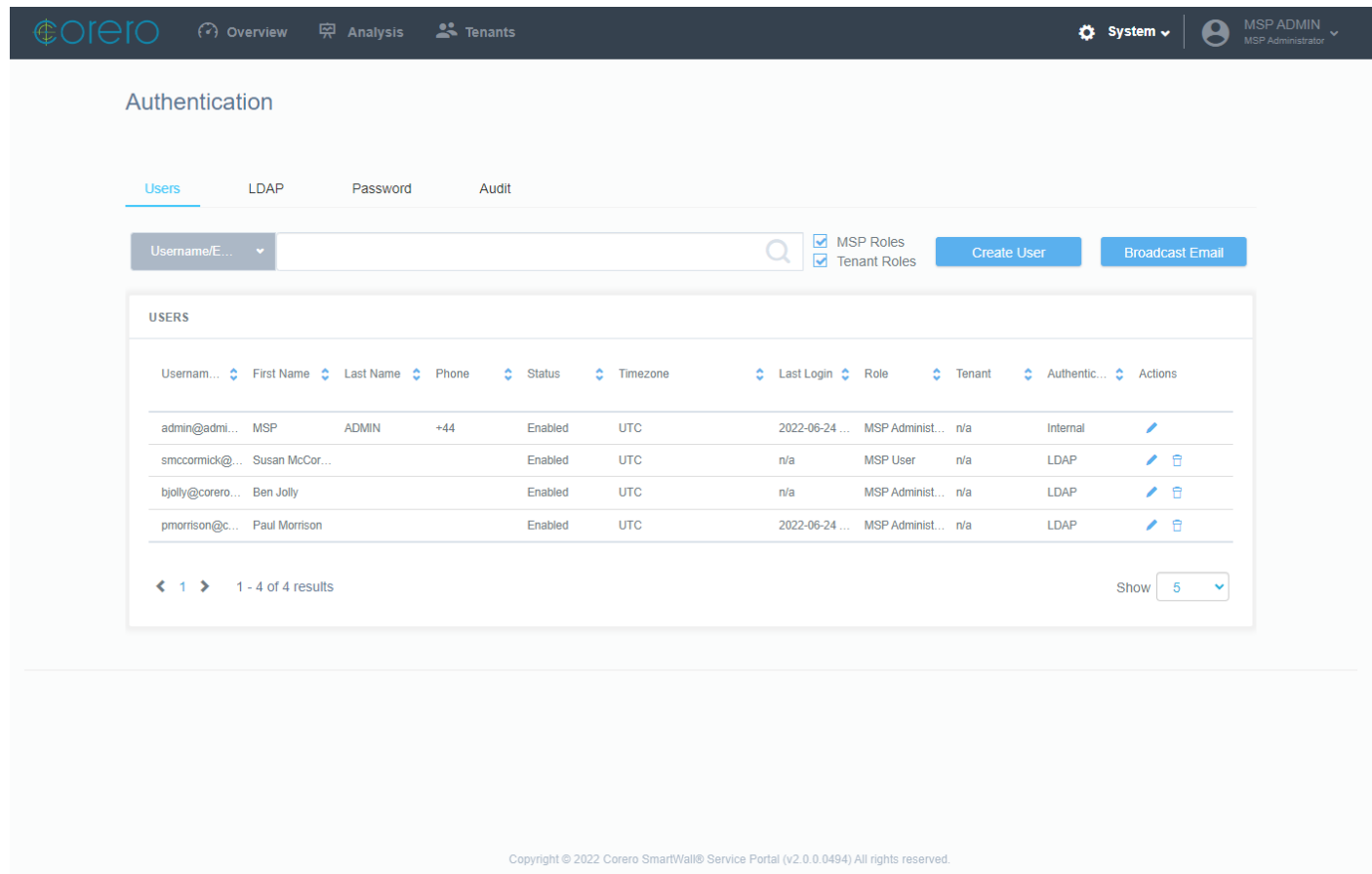
## LDAP Authentication

As well as creating local users, you can configure the Service Portal to accept externally authenticated users by connecting it to your organization's LDAP server (e.g. for use with Active Directory). Once you configure the Service Portal to connect, you can map LDAP groups on to the two user roles (MSP Administrator and MSP User) . For example, if you had an administrators group on the LDAP server, you could create a group mapping between that and the MSP Administrator role. Once you did that, any users in that LDAP group would be able to log onto the Service Portal using their existing organization credentials and have the same level of access that an MSP Administrator has.

**Caution:** If a user has both an LDAP authenticated account for the Service Portal and a local Service Portal user account, it can cause issues. After you configure LDAP authentication, you should disable or delete any local user accounts which are no longer required.

## Users Settings Screen

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



The screenshot shows the Corero Service Portal Admin Guide interface. The top navigation bar includes the Corero logo, tabs for Overview, Analysis, and Tenants, and a System dropdown menu. The System dropdown is open, showing the Users tab selected. The main content area is titled 'Authentication' and has tabs for Users, LDAP, Password, and Audit. The Users tab is active, displaying a search bar with a dropdown menu for 'Username/E...' and a search icon. Below the search bar are checkboxes for 'MSP Roles' and 'Tenant Roles', and buttons for 'Create User' and 'Broadcast Email'. A table titled 'USERS' lists user information with columns: Username, First Name, Last Name, Phone, Status, Timezone, Last Login, Role, Tenant, Authentication, and Actions. The table contains four rows of user data. At the bottom of the table, there is a pagination bar showing '1 - 4 of 4 results' and a 'Show' dropdown menu set to '5'.

Username	First Name	Last Name	Phone	Status	Timezone	Last Login	Role	Tenant	Authentication	Actions
admin@admi...	MSP	ADMIN	+44	Enabled	UTC	2022-06-24 ...	MSP Administ...	n/a	Internal	<a href="#">Edit</a>
smccormick@...	Susan McCor...			Enabled	UTC	n/a	MSP User	n/a	LDAP	<a href="#">Edit</a> <a href="#">Delete</a>
bjolly@corero...	Ben Jolly			Enabled	UTC	n/a	MSP Administ...	n/a	LDAP	<a href="#">Edit</a> <a href="#">Delete</a>
pmorrison@c...	Paul Morrison			Enabled	UTC	2022-06-24 ...	MSP Administ...	n/a	LDAP	<a href="#">Edit</a> <a href="#">Delete</a>



Copyright © 2022 Corero SmartWall® Service Portal (v2.0.0.0494) All rights reserved.

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

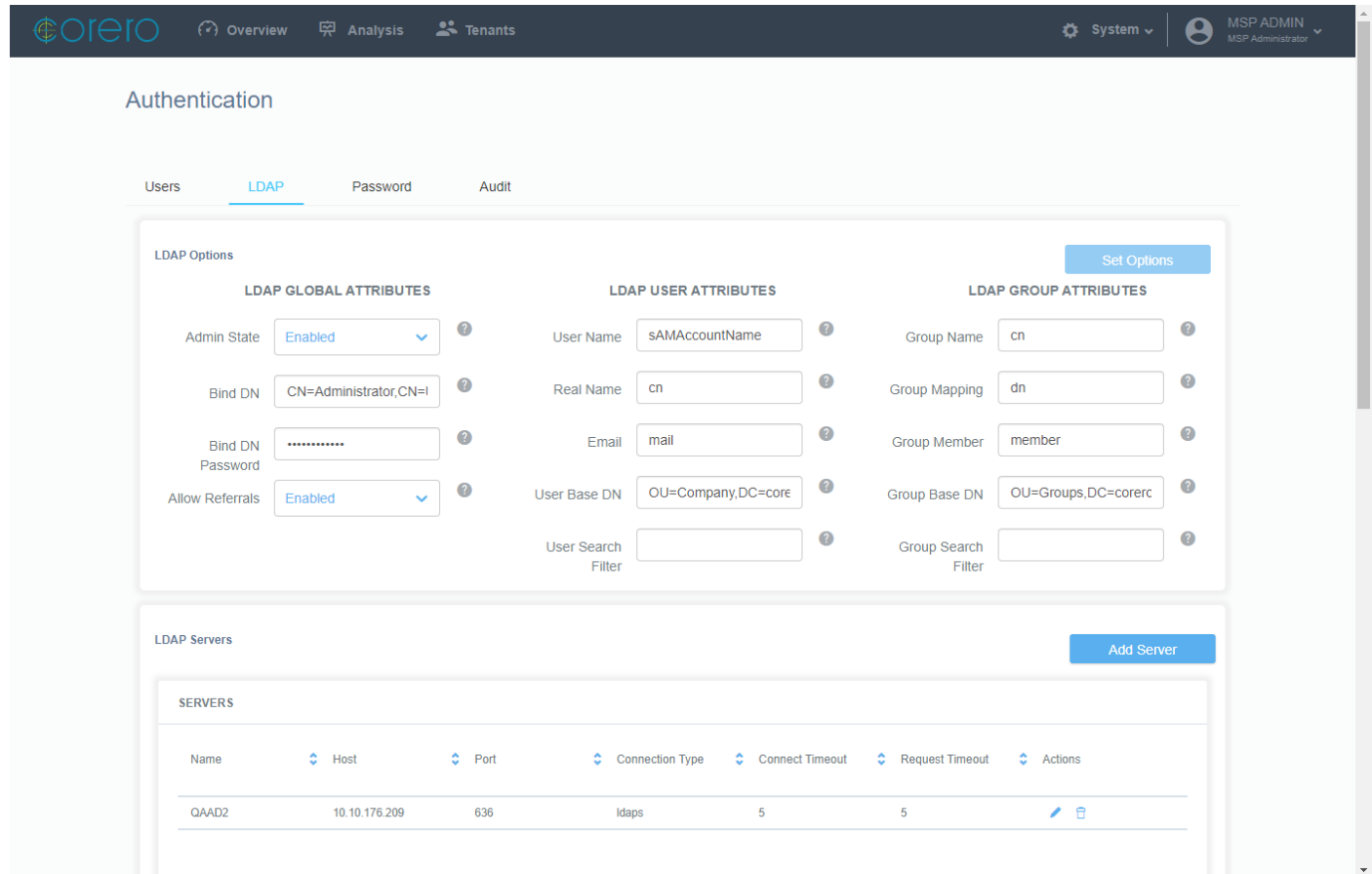
- **Timezone** – Select this option then, to filter the table to show users in one timezone, type the hours + or - from UTC for that timezone (i.e. +11)
- **Tenant Name** – Select this options then type all or part of a tenant name to view only the users in that tenancy.

The users 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: **MSP Administrator**, **MSP User**, **Tenant Administrator** or **Tenant User**
- **Tenant** – (Only relevant for Tenant Administrators and Tenant Users) The name of the tenancy this user belongs to.
- **Authentication** – Whether this user is **Internal** (created within the Service Portal) or **External** (authenticated via an LDAP server)
-  – Edit the selected user
-  – Delete the selected user

## LDAP Settings Screen

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



**Authentication**

Users **LDAP** Password Audit

**LDAP Options** Set Options

**LDAP GLOBAL ATTRIBUTES**

Admin State: Enabled ⓘ

Bind DN: CN=Administrator,CN=I ⓘ

Bind DN Password: ..... ⓘ

Allow Referrals: Enabled ⓘ

**LDAP USER ATTRIBUTES**

User Name: sAMAccountName ⓘ

Real Name: cn ⓘ

Email: mail ⓘ

User Base DN: OU=Company,DC=core ⓘ

User Search Filter:  ⓘ

**LDAP GROUP ATTRIBUTES**

Group Name: cn ⓘ

Group Mapping: dn ⓘ

Group Member: member ⓘ

Group Base DN: OU=Groups,DC=corerc ⓘ

Group Search Filter:  ⓘ

**LDAP Servers** Add Server

**SERVICES**



Name	Host	Port	Connection Type	Connect Timeout	Request Timeout	Actions
QAAD2	10.10.176.209	636	ldaps	5	5	<span></span> <span></span>

The LDAP Options section contains the following options:



- **LDAP Global Attributes:**
  - **Admin State** – Enables you to select whether LDAP authentication is **enabled** or **disabled**.
  - **Bind DN** – Enables you to type the username for a set of credentials which the Service Portal can use to retrieve user details from the LDAP server. They must have read access to the user store.
  - **Bind Password** – Enables you to type the password that corresponds to the Bind DN Username.
  - **Allow Referrals** – Enables you to select whether using LDAP referrals is **enabled** or **disabled**.

- LDAP User Attributes:
  - **User Name** – Enables you to type the LDAP attribute which contains the user's username.
  - **Real Name** – Enables you to type the LDAP attribute which contains the user's real name.
  - **Email** – Enables you to type the LDAP attribute which contains the user's email address.
  - **User Base DN** – Enables you to type the Base DN used to locate user information in the LDAP schema.
  - **User Search Filter** – (Optional) Enables you to type a filter to restrict user search results to a specific object class.
- LDAP Group Attributes:
  - **Group Name** – Enables you to type the LDAP attribute which contains the group's name.
  - **Group Mapping** – Enables you to type the LDAP attribute which group entries use to reference a group member.
  - **Group Member** – Enables you to type the LDAP attribute which contains a group member.
  - **Group Base DN** – Enables you to type the Base DN used to locate group information in the LDAP schema.
  - **Group Search Filter** – (Optional) Enables you to type a filter to restrict group search results to a specific object class.

The LDAP Servers table displays the following information for each server:

- **Name** – Displays the name of the LDAP server.
- **Host** – Displays the IP address of the server.
- **Port** – Displays the port number for this server.
- **Connection Type** – Displays the connection type: LDAP, LDAPS or Start-TLS
- **Connect Timeout** – Displays the maximum number of seconds the Service Portal is permitted to wait for a network response on connecting.
- **Request Timeout** – Displays the maximum number of seconds the Service Portal is permitted to wait for a network response on sending a request.
-  – Edit the selected server.
-  – Delete the selected server.

The Group Role Mapping table displays the following information for each mapping:

- **LDAP Group** – Displays the name of the LDAP Group.
- **Role** – Displays the Service Portal user role which this LDAP Group is mapped to.
-  – Edit the selected mapping.
-  – Delete the selected mapping.

The LDAP Synchronization section contains the following options:


- **Repeat every** – Enables you to select how often the Service Portal syncs with the LDAP server.
- **Start at** – Enables you to type the time for the first sync of the day.
- **Set Schedule** – Enables you to save the updated synchronization settings (in the Repeat every and Start at fields).
- **Sync Now** – Syncs the Service Portal to the current LDAP server state. Before the sync begins, a confirmation dialog appears which displays the numbers of new, updated, and deleted users that this operation will produce. You can click **OK** to complete the sync or **Cancel** to choose not to sync.

## Managing Users

From the [users 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. You can also manage your Tenant Administrators and Tenant users on the [Tenants screen](#).

**Caution:** If you only have one MSP Administrator account, you cannot delete it (or edit it to be a user account) until you have created a new administrator account.


### To create a new user


1. From the main toolbar of the Service Portal, click **System > Authentication**. You should see the **Users** tab.
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: MSP Administrator, MSP User, Tenant Administrator or Tenant User.
  - **Tenant** – (For Tenant Administrators and Tenant Users only) Select the name of the tenancy this user will have access to.
  - **Status** – By default **Enabled** is selected. You can select **Disabled** to create a disabled user account which you can later choose to enable.
4. Choose the type of first-time **Authentication** required by this user:
  - **Token** – Send the user a token they can use to access to the portal through the "Apply Password Token" link on the login page. Click **Generate** to create a token. Then you can either click **Copy** to save the token to your clipboard to send to the user using your own methods, or once you save the new user, you will have an Action button  on the user table to email the token directly to the user.
  - **Password** – Create a password for the user and repeat to **Confirm Password**. You will need to communicate this password to the user. They will be able to change this password later when they log in.

**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: \$@#!%\*?&^~.:(){}[]?.

5. **SSO Only** - select this option to restrict the user to using Single Sign-On for authentication.

**Note:** If you select this option, you do not need to assign a password or token to the user account.

6. (Optional) Type in a contact **Phone** number for the user
7. From the drop-down, select the **Timezone** this user is normally based in.
8. Select any of the **Suppress Emails** check boxes to stop the user receiving emails about specific alerts or reports.
9. Click **Save**.
10. (Optional) If you choose token authentication, you can now click  the send email button in the Actions column to send the authentication token to the user's email address. The content of the [Password Token email can be edited](#) (**System > Authentication > Password**).

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

### To unlock a user account

If a user has had their account locked, due to login mistakes for example, you can unlock the account from the users table.

The following user types can use this feature.

- MSP Admin can unlock any user
  - MSP User can unlock any tenant-admin or tenant-user
  - Tenant Admin can unlock any tenant-user
1. From the main toolbar of the Service Portal, click **System > Authentication**. You should see the **Users** tab.
  2. Locate the locked user in the table.
  3. In the actions column, click the unlock icon.

### To send an email to multiple users

**Note:** This feature is only available to MSP Admin users.

If you need to send a message to all Service Portal users, or a set of user types, you can send a Broadcast Email. This can be useful to warn of upcoming maintenance windows or site updates.

**Note:** Emails are send using BCC with the number of recipients per mail determined by [the Recipients Limit value in the email configuration](#) (**System > General Settings > Email**).

1. From the main toolbar of the Service Portal, click **System > Authentication**. You should see the **Users** tab.
2. Click **Broadcast Email**.
3. Use the **Broadcast to** check boxes to select which user groups you want to send this email to. By default, only MSP Admins and Tenant Admins are selected.
4. Type a **Subject** line for your email.



5. Type the **Email Body**. Select a section of the text and use the **B**, **I**, and **U** buttons to add formatting.
6. To check your email looks correct, click **Send me test mail**. A copy of your email will be sent just to your email address.
7. When you're happy with your email, click **Send** to send the email to all users in the selected user groups. Emails are sent immediately.

**Note:** You must have an [email server](#) configured on the Service Portal to send emails to users.

## Configuring LDAP Integration for Authentication Users

**Note:** Only MSP Administrators can configure this authentication method.

To enable your users to log into the Service Portal with their existing organization credentials, you can connect the Service Portal to your organization's LDAP server (e.g. Active Directory).

There are four main steps to connect an LDAP server to the Service Portal:

- Configure the LDAP attributes the Service Portal uses to identify users in your LDAP Server
- Add the connection details for an LDAP server to the LDAP Servers list. Optionally add a backup server.
- Create a group mapping for every LDAP group which needs to access the Service Portal and select the Service Portal user role that group will be provisioned with.
- Set up an LDAP synchronization schedule.

### To configure the CMS's LDAP attributes

1. From the main toolbar of the Service Portal, click **System > Authentication**. Then select the **LDAP** tab.
2. At the **Admin State** drop-down, make sure LDAP authentication is **enabled**.
3. Type in a **Bind DN** and **Bind DN Password** for a set of credentials which has read access to the user store.
4. Use the drop-down to decide if you will **Allow Referrals**. Note: allowing LDAP referrals can decrease performance.
5. Set the following LDAP User Attributes to identify users within the user store:
  - **User Name Attribute** – (Default: **sAMAccountName**) The LDAP attribute which contains the user's user-name
  - **Real Name Attribute** – (Default: **cn**) The LDAP attribute which contains the user's real name
  - **Email Attribute** – (Default: **mail**) The LDAP attribute which contains the user's email address
  - **User Base DN** – The Base DN used to locate user information in the LDAP schema
  - **User Search Filter** – Optional filter to restrict user search results to a specific object class
6. Set the following LDAP Group Attributes to identify groups within the user store:
  - **Group Name Attribute** – (Default: **cn**) The LDAP attribute which contains the group's name
  - **Group Mapping Attribute** – (Default: **dn**) The LDAP attribute which references a group member
  - **Group Member Attribute** – (Default: **member**) The LDAP attribute which contains a group member
  - **Group Base DN** – The Base DN used to locate group information in the LDAP schema
  - **Group Search Filter** – Optional filter to restrict group search results to a specific object class
7. Click **Set Options**.

**Note:** All LDAP User and Group Attributes are required unless listed as optional.

## To manage LDAP servers

**Note:** In addition to your primary LDAP server, you can add a backup server. The backup server must have the same Directory Information Tree structure as the primary LDAP server and accept the same bind credentials.

### To add an LDAP server

1. From the main toolbar of the Service Portal, click **System**. Then select the **LDAP** tab.
2. At the LDAP Servers table, click **Add Server**.
3. Type a **Name** for this server.
4. Select the **Connection Type** your LDAP server will use to communicate with the Service Portal.
5. Type the **Host** IP Address.
6. Type the **Port** number which corresponds with your connection type. By default, LDAP and Start-TLS use port **389** and LDAPS uses **636**.
7. Type a value for **Connect Timeout**. This is the maximum number of seconds the Service Portal is permitted to wait for a network response on connecting.
8. Type a value for **Request Timeout**. This is the maximum number of seconds the Service Portal is permitted to wait for a network response on sending a request.
9. Click **Save**.
10. (Optional) Repeat this method to add a back up server. You can only have two LDAP servers configured.

**Note:** You can edit  or delete  LDAP Servers from the LDAP Servers table.

## To manage group role mappings

There are 2 Service Portal user roles you can map an LDAP group to. User's in a mapped group will have the same permissions as their associated role:



- **MSP Administrator** – Can view traffic data, analyze attacks, manage tenants, manage other MSP Administrators and MSP Users, edit Service Portal system settings
- **MSP User** – Can view traffic data, analyze attacks and manage tenants

**Note:** You can map multiple LDAP groups to each user role.

### To add a group role mapping

1. From the main toolbar of the Service Portal, click **System**. Then select the **LDAP** tab.
2. At the Group Role Mapping table, click **Add Mapping**.
3. Type the name of an **LDAP Group** from your user store.

4. Select the **Role** you want to map to that group.
5. Click **Save**.

**Note:** You can edit  or delete  group role mappings from the Group Role Mapping table.

### To set an LDAP synchronization schedule

The Service Portal should update the lists of external users and their roles periodically to make sure they always have the most up to date access.

**Tip:** To quickly sync the Service Portal and the LDAP server without waiting for the scheduled time, click **Sync Now**.

1. From the main toolbar of the Service Portal, click **System**. Then select the **LDAP** tab.
2. In the LDAP Synchronization sections, use the **Repeat every** drop-down to select how often the Service Portal should sync with the LDAP server.
3. In the **Start at** field, type the time you want to perform the first sync of the day.
4. Click **Set Schedule**. Once you sync, you can see a summary of the **Last Sync Attempt**.

### Configuring Single Sign-On

**Note:** Only MSP Admin users can configure SSO authentication.

Single Sign-On (SSO) allows users of the Service Portal to log in to the application with a set of credentials provided by a nominated external identity provider (IDP). To configure this feature, you must first have registered with an IDP who provides an OpenConnect ID compliant authorization service. Your IDP will then provide the necessary details to allow you to configure SSO for the Service Portal.

The following considerations apply to SSO authentication:

- Only existing users of the Service Portal can use SSO authentication.
- SSO may be configured as a mandatory method of authentication by enabling the **SSO Only** option when creating or amending a user account.
- If SSO is not configured as mandatory for a user, they can continue to use their existing account name and password to log in to the application. If it is configured, the regular (non-SSO) credentials are ignored and do not need to be entered.

- The example configuration details shown here are based on the Azure Active Directory (Azure AD) and Okta IDPs. Other IDPs may require different configuration parameters. For example, SSO will require your IDP to return the email address of an authenticated user. Some IDPs will return this automatically, some will require some configuration to do this and some will require an additional scope parameter to be presented to retrieve this information. Please check with your IDP to determine exactly what setup is required before you begin configuration.
- Only IDPs which support the industry-standard OpenConnect ID protocol for identity verification may be used to provision SSO in the Service Portal.

## To Access Single Sign-On Configuration

In the main toolbar, click **System** > **Authentication** > **Single Sign-On** to display the Single Sign-On Configuration tab.

### Example #1 - Azure AD

### Single Sign-On Configuration

Reset configuration

Single Sign-On will require your identity provider to return the email address of an authenticated user. Some identity providers will return this automatically, some will require some configuration to do this and some will require an additional scope to be presented to retrieve this information. Please check with your identity provider to determine what setup is required.

Admin State \* ? Enabled

Name \* ? example\_sso

Client ID \* ? 6a913068-aaf3-4c7d-8bf1-d28e6266fcf6

Client Secret \* ? .....

Issuer URI \* ? https://login.microsoftonline.com/82495eca-f1b2-4d30-adf8-cc4d43

Additional Scopes ?

Disable user creation for tenant administrators \* ? No

Save

## Example #2 - Okta

Single Sign-On Configuration

Reset configuration

Single Sign-On will require your identity provider to return the email address of an authenticated user. Some identity providers will return this automatically, some will require some configuration to do this and some will require an additional scope to be presented to retrieve this information. Please check with your identity provider to determine what setup is required.

Admin State \* ?

Enabled

Name \* ?

oktaexample

Client ID \* ?

6a913068-aaf3-4c7d-8bf1-d28e6266fcf6

Client Secret \* ?

.....

Issuer URI \* ?

https://dev-9734306.okta.com

Additional Scopes ?

email

Disable user creation for tenant administrators \* ?

No

Save

Single Sign-On Configuration tab allows you to enter the SSO configuration details for the IDP you have registered with, and enable or disable SSO in the Service Portal. You can also use this tab to subsequently amend the configuration details if required.

The following data fields are available (required fields are marked with an asterisk (\*)):

**Admin State** – A required parameter which controls whether or not SSO is enabled in the Service Portal. If **Enabled**, users will see a **Or log in with Single Sign-On** link on their login screen, in addition to the normal **Username** and **Password** entry fields. Selecting **Disabled** will remove the **Or log in with Single Sign-On** link for all users.

**Name** – A required human-readable name which will identify the SSO configuration. This is used for display purposes only.

**Client ID** – A required field which must contain the Client ID (a service account username supplied by your IDP) which is used to log in securely to the external IDP service.

**Client Secret** – A required field which must contain the Client Secret (a service account password supplied by your IDP) which is used to log in securely to the external IDP service. It will be hidden in the tab when you next sign in to the Service Portal, however unless you make any changes to this field, you do not have to re-enter the Client Secret when updating the configuration.

**Issuer URI** – A required field which must contain the Uniform Resource Identifier (URI) supplied by your IDP. This is used internally by the Service Portal to locate specific information which the IDP service provides.

**Additional Scopes** - An optional, comma-separated list of scope names which represent specific information to be retrieved from the IDP service. These are based on the OpenConnect ID protocol standards, and will vary from one provider to another. The scope `openid` is included automatically and does not need to be entered. If your IDP service does not automatically return an email address for authenticated users, for example, adding the scope name `email` may allow this information to be returned.

**Disable user creation for Tenant Administrators** – A required field which specifies whether or not Tenant Administrators can create user accounts after SSO is enabled.

Click **Save** to complete the process once you have entered the information above. You can also click **Reset configuration** if you wish to clear all the configuration details and start again.

**Caution:** If you reset the configuration, all details will be deleted from the Service Portal, including the Client Secret. If you did not note this value separately, you will need to obtain a new Client Secret from your IDP before creating a new configuration.

## Enabling SSO Authentication

Once you have created a valid SSO configuration, you can enable it for use in the Service Portal by selecting **Yes** in the **Enabled** drop-down list on the Single Sign-On Configuration tab.

The first time you enable SSO authentication, you will see the following banner appear on the tab:

- ☐ Single sign-on will be accessible at [https://10.10.244.107/sso/example\\_sso](https://10.10.244.107/sso/example_sso)
- ☐ You will need to ensure your identity provider is using the redirect URI [https://10.10.244.107/sso-callback/example\\_sso](https://10.10.244.107/sso-callback/example_sso)

This banner provides a reference to the authentication URI which will be used to display the user authentication page (the appearance of which will vary depending on your IDP), and a callback URI which you will need to supply to your IDP to redirect users back to the Service Portal after authentication. You can copy either of these URIs to the clipboard by clicking the ☐ Copy to clipboard icon.

## Password Settings

**Note:** This feature is only available to MSP Admin users.

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

**Note:** Password expiry options apply to all MSP Administrators, MSP Users, Tenant Administrators, and Tenant Users associated with your Service Portal, unless overridden at a Tenant level.

### 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 to have the password reset.

### Per-Tenant password expiry options

You can override the system-wide password expiry options for specific tenants. When you select a tenant on the **Tenants** screen, you can view the **Password** tab. The options here enable you to override the system-wide settings and provide settings specific for this tenant. You can also choose to allow the Tenant Administrators to manage these options themselves for their tenancy.


### Password Email Templates

Creating, resetting, or changing expired/nearly expired passwords all require sending an email to the user. The Service Portal has default email text for each of these actions, but you can choose to customize this text to match your company style.

### Password Settings Screen

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




Overview
Analysis
Tenants
System
MSP ADMIN

## Authentication

Users
LDAP
Password
Audit

### OPTIONS

Passwords expire after  days

Password expiration warning period  days

Password change grace period  days





Onscreen password notifications ☒

Email password notifications ☒

Send password email notifications at

Save

### EMAIL TEMPLATES

Type	Actions
Password Token	
Password Reset	
Password Expiration Warning	
Password Expired	

Copyright © 2022 Corero SmartWall® Service Portal (v2.0.0.0494) All rights reserved.

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.

You can customize the following Email Templates:

- **Password Token** – This email is sent to a new user when the Administrator has [selected Token authentication](#) during user creation and chosen to send the authentication email.
- **Password Reset** – This email is sent when a user has requested a new password using the **Forgot Password?** option on the Service Portal login screen.
- **Password Expiration Warning** – This email is sent during the user's password expiry warning period.
- **Password Expired** – This email is sent during the user's password change grace period.

## Managing Password Expiry Options

You can change the password expiry options for all users on the portal.

### *To edit the system-wide password expiry options*

These changes apply to MSP Administrators and MSP Users. They also apply to all Tenant Administrators and Tenant Users, unless their tenancy has its own password expiry options configured.

1. From the main toolbar of the Service Portal, click **System > Authentication**, 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 expiry the Service Portal should begin warning the user.
  - **Password change grace period** – (Default: 4 days) Type how many days after expiry 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.

### *To edit the password expiry options for a specific tenant*

These changes only apply to the Tenant Administrators and Tenant Users in this tenancy.

1. From the main toolbar of the Service Portal, click **Tenants**.
2. Select a Tenant from the list, then click the **Password** tab.
3. To set tenant specific options, select the check box next to **Override System Settings**.
4. (Optional) If you want to allow the Tenant Administrators in this tenancy to manage their own Password Expiry settings, select the box next to **Permit Tenant Administrator Modification**. If you do, Tenant Administrators will see a Password tab in their System Settings screen.
5. You can edit the following options for this tenancy:


6.
  - **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 expiry the Service Portal should begin warning the user.
  - **Password change grace period** – (Default: 4 days) Type how many days after expiry 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 email 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.
7. When you're happy with the settings, click **Save**.

## Editing Password Email Templates

**Note:** Only MSP Administrators can edit these templates.

There are multiple types of password email which can be generated by the Service Portal to help users manage their passwords. These emails can be customized by editing the email template for each email type.

### *To edit an email template*

1. From the main toolbar of the Service Portal, click **System > Authentication**, then the **Password** tab.
2. Click  the edit button next to the email template you want to edit:
  - **Password Token** – This email is sent to a new user when the Administrator has [selected Token authentication](#) during user creation and chosen to send the authentication email.
  - **Password Reset** – This email is sent when a user has requested a new password using the **Forgot Password?** option on the Service Portal login screen.
  - **Password Expiration Warning** – This email is sent during the user's password expiry warning period.
  - **Password Expired** – This email is sent during the user's password change grace period.
3. Edit the example **Subject** line for the email.

**Tip:** \u2013 in the example Subject field is replaced with a copyright symbol when the email is sent.

4. Edit the example **Body** to change the content of the email. Select a section of the text and use the **B**, **I**, and **U** buttons to add formatting. The following placeholders can be used for each template:

- **Password Token:**
  - `${userName}` – Replaced with the first and last name of the user (e.g. Joe Bloggs ).
  - `${token}` – Replaced with the unique password token required by this user.
- **Password Reset:**
  - `${userName}` – Replaced with the first and last name of the user (e.g. Joe Bloggs ).
  - `${token}` – Replaced with the unique password token required by this user.
- **Password Expiration Warning:**
  - `${userName}` – Replaced with the first and last name of the user (e.g. Joe Bloggs ).
  - `${expireAfter}` – Replaced with the time remaining until password expiry (e.g. in 15 days, today ).
  - `${gracePeriod}` – Replaced with the length of the grace period (e.g. 4 days ).
- **Password Expired:**
  - `${userName}` – Replaced with the first and last name of the user (e.g. Joe Bloggs ).
  - `${accountDisable}` – Replaced with the time remaining until the account is disabled at the end of the grace period (e.g. in 4 days, today ).

5. Click **Save**.

## User Audit Log

To view user activity on your SmartWall Service Portal you can use the audit log to see a list of every user action performed on the portal. This includes both tasks performed by MSP Administrators and MSP Users on your provider portal, and tasks performed by Tenant Administrators and Tenant Users on their own tenant portals.

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.

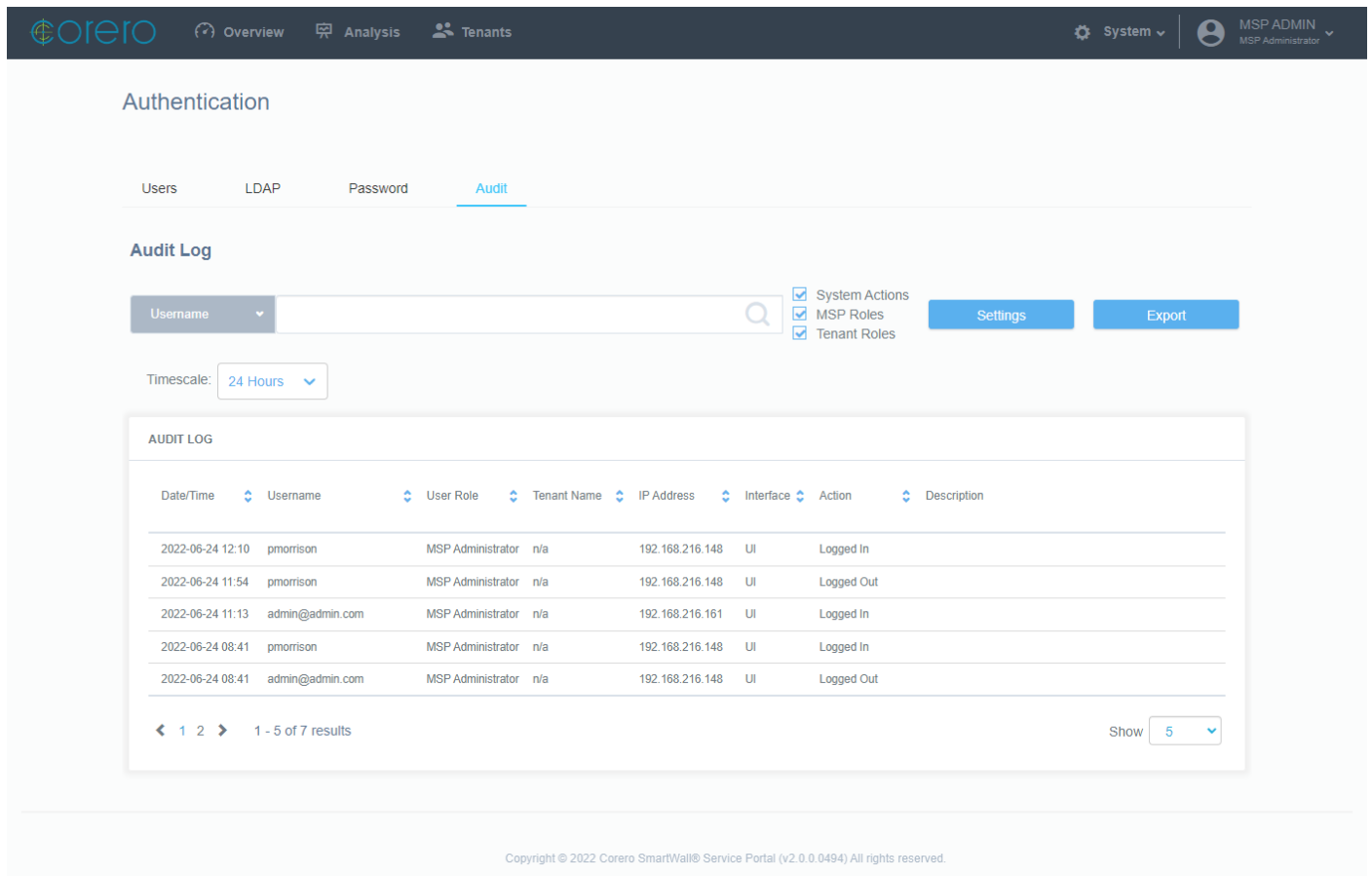
What you see on the audit log depends on your User Role:

- An MSP Administrator can see every action performed by other MSP Administrators, all MSP Users, all Tenant Administrators and all Tenant Users.
- An MSP User can see every action performed by all Tenant Administrators and all Tenant Users.

**Note:** In the Tenant's portal view, a Tenant Administrator can see an audit log of what has happened on their own tenancy. This includes changes made by MSP Administrators and MSP Users, but the Username and IP Address are not shown for these changes.

## Audit Settings Screen

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



The screenshot shows the Corero Service Portal Admin Guide interface. At the top, there is a navigation bar with the Corero logo, links for Overview, Analysis, and Tenants, and a System menu. The main content area is titled 'Authentication' and has tabs for Users, LDAP, Password, and Audit. The Audit tab is selected, showing an 'Audit Log' section. This section includes a search bar with a dropdown for 'Username' and a search icon. To the right of the search bar are three checkboxes: 'System Actions', 'MSP Roles', and 'Tenant Roles', all of which are checked. Below the search bar is a 'Timescale' dropdown set to '24 Hours'. To the right of the search bar are two buttons: 'Settings' and 'Export'. Below these elements is a table titled 'AUDIT LOG' with columns: Date/Time, Username, User Role, Tenant Name, IP Address, Interface, Action, and Description. The table contains five rows of data. At the bottom of the table, there is a pagination bar showing '1 - 5 of 7 results' and a 'Show' dropdown set to '5'.

Date/Time	Username	User Role	Tenant Name	IP Address	Interface	Action	Description
2022-06-24 12:10	pmorrison	MSP Administrator	n/a	192.168.216.148	UI	Logged In	
2022-06-24 11:54	pmorrison	MSP Administrator	n/a	192.168.216.148	UI	Logged Out	
2022-06-24 11:13	admin@admin.com	MSP Administrator	n/a	192.168.216.161	UI	Logged In	
2022-06-24 08:41	pmorrison	MSP Administrator	n/a	192.168.216.148	UI	Logged In	
2022-06-24 08:41	admin@admin.com	MSP Administrator	n/a	192.168.216.148	UI	Logged Out	

Copyright © 2022 Corero SmartWall® Service Portal (v2.0.0.0494) All rights reserved.

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
- **Tenant Name** – To find all actions performed within a specific tenancy
- **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
- **Interface** – To find all actions performed using the UI or REST API
- **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)

- **MSP Roles** – Show or hide all actions performed by MSP Administrators and MSP Users
- **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, and the **Settings** button, which you can use to manage the Maximum age of portal and tenant log entries.

**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
- **Tenant Name** – The tenancy in which this action was performed
- **IP Address** – The IP address from which the user accessed the Service Portal
- **Interface** – Whether this action was performed using the UI or the REST API
- **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 > Authentication**.
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.

## Managing Audit Log Rotation

You can choose how long the Audit Log stores entries for actions made by MSP Administrators and MSP Users on the portal, and how long it stores entries for actions made by Tenant Administrators and Tenant Users on their own tenancies.

### *To manage Audit Log rotation*

1. From the main toolbar of the Service Portal, click **System > Authentication**.
2. Open the **Audit** tab..
3. Click **Settings**.
4. Edit the following settings:
  - **Maximum age of portal log entries** – The number of days you want the audit log to store portal user actions before they are deleted
  - **Maximum age of tenant log entries** – The number of days you want the audit log to store tenant user actions before they are deleted
5. Click **Save**.

## Managing REST API Tokens

**Note:** Only MSP Administrators users can manage tokens. Tokens may only be used to authenticate external REST API calls. They cannot be used to log in to the Service Portal user interface.

In addition to standard user credentials, tokens may be used for authenticating REST API calls to the Service Portal. This is a more reliable and secure form of authentication, as it avoids the possibility of credentials expiring over time.

In the Service Portal, you can create, revoke and review tokens directly in the user interface.

For more information on how to use REST API tokens in other applications, see [REST API Overview](#).

### To create a REST API token


1. From the main toolbar of the Service Portal, click **System > Authentication > API Tokens**.
2. On the API Tokens panel, click **Generate new token**.



The image shows a 'Generate API Token' dialog box. It has a title bar with a close button (X). Inside, there are two required fields: 'Name \*' with a question mark icon and a text input containing 'CSM01'; and 'Role \*' with a question mark icon and a dropdown menu showing 'MSP User'. At the bottom right, there are two buttons: 'Cancel' and 'Generate'.

3. Type an identifying **Name** for the token.


**Note:** The token name will appear in the Username column of the [audit log](#) for any associated updates made via the REST API.

4. From the drop-down list, select a suitable user **Role**.
5. Click **Generate**.
6. Once the token has been generated, it will appear in the API Tokens list. You should now copy the generated token value by clicking  the Copy to clipboard icon.

**Note:** You can only copy the generated token value once. You should copy it immediately before clicking away from the panel. Token values cannot be redisplayed at a later date.

- Once you have copied the token value to the clipboard, you can distribute it as required according to the security protocols mandated by your organization.



### To revoke a REST API token



- From the main toolbar of the Service Portal, click **System > Authentication > API Tokens**.
- On the API Tokens panel, locate the token you wish to revoke in the displayed list, and then click  the Revoke button.
- Click **OK** in the confirmation dialog, or click **Cancel** to abandon the operation.


**Note:** Revoked tokens will be permanently deleted from the API Tokens list, and any future REST API calls using the revoked token will fail authentication.

### To review existing REST API tokens

- From the main toolbar of the Service Portal, click **System > Authentication > API Tokens**.
- On the API Tokens panel, you will see a list of all tokens currently in use, and the date the token was last used (if any).

API TOKENS				
Name	Role	Last Used	Created	Actions
CMS01	MSP User	n/a	2022-10-19 14:30	
SWA01	MSP User	n/a	2022-10-19 14:31	



1 - 2 of 2 results

Show
5


## Policy and Reporting

This section enables you to configure Service Levels and Reporting for the Service Portal.

### Service Policy and Alerting

**Note:** Only MSP Administrators users can configure Service Levels.

When providing DDoS protection to your tenants, the Service Portal has the flexibility to match how you decide to offer your DDoS protection-as-a-service, with automated reporting and alerting. This is applied through the use of Service Levels.

#### Service Levels

You can create as many Service Levels as you need.

There are 2 ways you can choose to use Service Levels:

- Rate-based service policy – Created and managed in the Service Portal.
- Rule-based service policy – Using the Service Levels already created, plus additional functionality for modifying rule actions which are managed in the SWA.

#### *Rate-based service policy*

For each service level, you can optionally set a **maximum mitigation rate** (between 0-1000Gbps). For example, you might choose to set up three service levels - Bronze, Silver, and Gold - where each level has an increasing maximum mitigation amount. Your customers can then choose the service level that is right for them, depending on the type of attacks they normally experience. If an attack on a tenant exceeds their maximum mitigation rate it produces an alert in the system which you can use to send an email alert.

**Tip:** Set up a basic Service Level enabling you to send alerts to any unsubscribed customers when they are attacked, Allowing the discussion about subscription options that you can offer them.

#### *Rule-based service policy (TDD deployments only)*

After creating your Service Levels in the Service Portal, a Rule-based service policy configuration can be managed on the SWA application of your TDD system. The SWA pulls your service level configuration from the Service Portal. Then, for each service level, it enables you to make modifications to the default rule actions, of the defense policy used by the TDD system, to identify and block attack traffic.

For example, a customer paying for a higher tier service level may get all of the TDD Smart-Rules set to block attack traffic by default, but a lower tier customer may have them set to only detect attack traffic. As well as choosing to block or detect traffic, you can use the policer action to limit the rate of attack traffic, matching rules a customer can

have, and the redirect action to re-route the traffic matching that rule. See the SmartWall TDD User Guide for full configuration instructions.

## Alerts

Alerts are notifications sent to users of the Service Portal to inform them of specific system events. All users will receive email alert notifications if this is configured for their specified service level, although you can suppress specific alert types on an individual user's account which will prevent them from receiving those alerts.

In addition, the Service Portal can send email and/or Webhook alert notifications to any specified destination, including external recipients. This method of alert notification is recommended, as it allows alerts to be sent to distribution lists, email groups and Slack/Microsoft Teams channels without the need to create user accounts simply for notification purposes. See [Notification Settings](#) for more information on this feature.

For every service level, you can choose to configure any of these alert types:

- **Service level alerts** – The Service Portal sends an alert to the selected recipients when a tenant exceeds this service level's maximum mitigation rate.
- **Attack status alerts** – The Service Portal sends an alert to the selected recipients when an attack starts or stops against a tenant on this service level. Attack status alerts are sent per attacked DIP (for the first 5 DIPs in an attack) or per attacked Assigned Asset (if there are more than 5 DIPs targeted).
- **Remote Mitigation alerts** – The Service Portal sends an alert to the selected recipients when a tenant is subject to [Remote Mitigation](#).

**Note:** You can choose to [suppress alerts for specific users](#) if you don't want them to receive the notifications.

When you configure a service level's alerts, you can select the type of users who will receive the notification and you can define content for the subject and body. You can include placeholder fields; these instruct the Service Portal to insert changeable information before it sends the alert. You can use the following placeholders:

**Note:** For attack status alerts, the attack specific placeholders (e.g. `attack_id`) provide information on the attack associated with this alert, and for service level alerts, the attack specific placeholders provide information on the attack which caused the service level to be exceeded.

## Service Level and Attack Status alerts

- **{alert\_timestamp}** – Inserts the time and date of the alert. It should look similar to this example: 4 Jan 2020 18:25:00 UTC

- **{service\_level}** – Inserts the name of the service level the tenant associated with this alert subscribes to, as it is displayed in the Policy table
- **{max\_mitigation}** – Inserts the maximum mitigation rate (in Gbps) associated with the service level. For amounts over 1Gbps this is displayed in whole numbers and for amounts less than 1Gbps it displays to one decimal place.
- **{attack\_id}** – Inserts the unique identification number of the attack which triggered the alert. If there are 5 or less descriptions, they are all shown separated by ‘;’ otherwise the following text is added: “Multiple attack IDs” .
- **{attack\_description}** – Inserts a description of the attack which triggered the alert. It should appear similar to the following example:  
 Finished attack to 10.199.250.181 for 7 minutes. Attack vector: Reflective 52318 to service Battlefield ( 25200/udp ) Reflective 56116 to service Battlefield ( 25200/udp ) Service Flood to Battlefield ( 25200/udp ) Service Flood to Battlefield ( 25200/udp ) . Max Values: 12922850 pps / 6614 Mbps . Rules triggered: cns-002023 cns-002033 cns-002037 cns-002057 cns-002023 cns-002033 cns-002057 cns-002033  
 If there are 5 or less descriptions, they are all shown separated by ‘;’ otherwise the following text is added: “Multiple attack vectors”.
- **{attack\_status}** – Inserts the current status of the attack at the time of the alert. For service level alerts, this can be started or ongoing. For attack status alerts, this can be started or completed.
- **{attack\_start\_time}** – Inserts the time and date when the attack began. It should look similar to this example: 4 Jan 2020 18:25:00 UTC. For multiple DIPs under attack, this is the earliest start time.
- **{attack\_duration}** – Inserts the number of seconds between the beginning of the attack (the attack\_start\_time) and either the end of the attack for completed attacks, or the time the alert was generated for on going attacks (the attack\_event\_time). For example: 420
- **{attack\_ip}** – Inserts the Assigned Asset which contains the target of this attack. If less than 5 DIPs are under attack, they are listed in brackets after the assigned asset. If more than 5 DIPs are under attack, this is shown by showing "Multiple IPs) in the brackets. For example:
  - “192.168.1.0/24 (IP: 192.168.1.1)”
  - “192.168.1.0/24 (IP: 192.168.1.1, 192.168.1.100)”
  - “192.168.1.0/24 (Multiple IPs)”
- **{attack\_event\_time}** – Inserts the time of the last attack event or status change. If an attack is completed, this is the same as the end time. It should look similar to this example: 4 Jan 2020 18:25:00 UTC. For multiple DIPs under attack, this is the latest event time.
- **{attack\_max\_bitrate}** – Inserts the maximum rate of attack traffic seen by the Assigned Asset during this attack (in Mbps). It should look similar to this example: 6614
- **{attack\_volume}** – Inserts the volume of traffic sent over the duration of the attack.

- **{tenant\_name}** – Inserts the name of the tenant associated with this alert, as it is displayed in the Tenants table. For service level alerts, this is the tenant whose attack traffic has exceeded their max mitigation value and for attack status alerts, this is the tenant associated with the destination IP address which is under attack.
- **{tenant\_identifier\_1}** – If this field is populated in the Tenant's details, inserts the Tenant Identifier 1 value. For example: Customer 3203
- **{tenant\_identifier\_2}** – If this field is populated in the Tenant's details, inserts the Tenant Identifier 2 value. For example: Customer 3203

### Remote Mitigation alerts

- **{remote\_mitigation\_type}** – Inserts the type of remote mitigation applied to the tenant.
- **{remote\_mitigation\_status}** – Inserts the current status of the remote mitigation at the time of the alert. This can be started, ongoing, or completed.
- **{remote\_mitigation\_start\_time}** – Inserts the time and date when the remote mitigation began. It should look similar to this example: 4 Jan 2020 18:25:00 UTC.
- **{remote\_mitigation\_impacted\_ip}** – Inserts the Tenant's IP addresses which are impacted by this remote mitigation.
- **{remote\_mitigation\_duration}** – Inserts the number of seconds between the beginning of the remote mitigation (the remote\_mitigation\_start\_time) and either the end of the remote mitigation for completed events, or the time the alert was generated. For example: 420
- **{tenant\_name}** – Inserts the name of the tenant associated with this alert, as it is displayed in the Tenants table.
- **{asset\_ip}** – Inserts the IP range of the asset which is affected by the remote mitigation.
- **{asset\_name}** – Inserts the name of the asset which is affected by the remote mitigation.

#### *Example service level alert message*

Subject:

DDoS attack targeting **{tenant\_name}** exceeded service level

Body:

A DDoS attack against **{tenant\_name}**, which started at **{attack\_start\_time}** has exceeded the current **{service\_level}** service level. The attack generated **{attack\_max\_bitrate}**Mbps of traffic which is greater than your current maximum mitigation size of **{max\_mitigation}**Gbps.

#### *Example attack status alert message*

Subject:

DDoS attack **{attack\_status}** targeting **{tenant\_name}**

Body:

A **{tenant\_name}** asset (**{attack\_ip}**) is the target of a DDoS attack which started at **{attack\_start\_time}**.

The following is a summary of the attack:

**{attack\_description}**

You can view more information about this specific attack on the service portal Attack Analysis screen, using the following Attack ID in the search bar drop-down: **{attack\_id}**

## Service Policy and Alerting screen

You can navigate to the Service Policy and Alerting screen by clicking **System** on the main toolbar then the **Policy** tab.

[Create Service Level](#)

**SERVICE POLICY AND ALERTING**

Service Level	Max Mitigation (Gbps)	Description	Service Level Alerts	Attack Status Alerts	Remote Mitigation Alerts	Actions
Level-1	500		Enabled	Enabled	Enabled	<a href="#">✎</a> <a href="#">🗑</a>
Level-2	250		Disabled	Disabled	Disabled	<a href="#">✎</a> <a href="#">🗑</a>
Level-3	100		Disabled	Disabled	Disabled	<a href="#">✎</a> <a href="#">🗑</a>

◀ 1 ▶ 1 - 3 of 3 results
Show 5 ▼



Webhook Alerts Enabled ▼

When you install the Service Portal you can use this screen to set up your service policy. After that you can return here to view or edit that configuration.

The policy table contains the following information for each Service Level:

- **Service Level** – The name of this Service Level
- **Max Mitigation** – The maximum rate of attack mitigation allowed on this Service Level (in Gbps)
- **Description** – An optional description of the Service Level
- **Service Level Alerts** – Whether Service Level alerts are **enabled** or **disabled** for this Service Level
- **Attack Status Alerts** – Whether Attack Status alerts are **enabled** or **disabled** for this Service Level
- **Remote Mitigation Alerts** – Whether Remote Mitigation alerts are **enabled** or **disabled** for this Service Level



-  – Edit the selected Service Level
-  – Delete the selected Service Level

**Note:** For MSP Users, the action buttons are not available, as they can only view the Service Levels.

You can globally disable **Webhook Alerts** from this screen using the drop-down. By default, Webhook alert notifications are enabled. Disabling Webhook notifications hides the Webhook panel from the Notifications tab in both the Policy and Reporting screen and the Tenant Management screen. Alert types can still be enabled (or disabled) when you create or amend a Service Level, to enable configuration, but Webhook alert notifications will not be sent while they are globally disabled.

### Configuring Service Levels and Alerts

Once you chose a subscription structure for your tenants, you'll need to configure the SmartWall Service Portal's policy to reflect the Service Levels you want to offer. Once you have set up a service level policy, when you [create a tenant](#), you can now select a Service Level.

**Note:** If you have a TDD system and choose to provide a Service Level policy which offers different attack mitigation options for each Service Level, you must enable syncing with the SWA application, and use the SWA Web UI to configure modify the default rule actions for each Service Level. See the SmartWall TDD User Guide for more information.

#### *To create a new Service Level*

**Note:** You must have an [email server](#) configured on the Service Portal to send emails to users. You must have a [Webhook](#) configured to send Slack or Teams messages to MSP Admin and Users. Tenant Admins can configure their own Webhooks to receive alerts sent to Tenant Channels.



1. From the main toolbar of the Service Portal, click **System > Policy and Reporting**, then select the **Policy** tab.
2. Click **Create Service Level**.
3. On the **General** tab, complete the following fields:
  - **Service Level** – Type a name for this Service Level
  - **Max Mitigation (Gbps)** – Type the maximum attack mitigation rate for a tenant on this Service Level in gigabits per second
  - **Description** – (Optional) Type a description of the Service Level.

4. There are three types of alerts which can be configured for each Service Level:
- **Service Level Alerts** – If you want users to be alerted when a tenant exceeds this Service Level's max mitigation rate.
  - **Attack Status Alerts** – If you want users to be alerted when a tenant on this Service Level experiences an attack.
  - **Remote Mitigation Alerts** – If you want users to be alerted when a tenant on this Service Level experiences a Remote Mitigation.

5. For each alert type you can enable **Email Alerts** and/or **Webhook Alerts**:

- To enable an email alert:
  - a. **Email alerts** – By default alerting is **Disabled** for a new Service Level, to start using alert emails, select **Enabled**
  - b. **Subject** – Edit the example subject line for the alert email. You can use the **Placeholder** drop-down to add changeable text fields to the subject line. When the email is sent, the Service Portal populates the placeholder field with the relevant information.
  - c. **Email Body** – Edit the example contents of the alert email. Select a section of the text and use the **B**, **I**, and **U** buttons to add formatting. You can also use the **Placeholder** drop-down to add changeable text fields to the body of the email. When the email is sent, the Service Portal populates the placeholder field with the relevant information
  - d. **Alert to** – Use the check boxes to select which users you want to send the email alert to:
    - **MSP Admins** – (By default this is the only box selected) All MSP Admins in the Service Portal
    - **MSP Users** – All MSP Users in the Service Portal
    - **Tenant Admins** – The Tenant Admins for a tenancy, on this Service Level.
    - **Tenant Users** – The Tenant Users for a tenancy, on this Service Level.
- To enable a webhook alert:
  - a. **Webhook alerts** – By default alerting is **Disabled** for a new Service Level, to start using Webhook alerts, select **Enabled**
  - b. **Header** – Edit the example header line for the Webhook alert. You can use the **Placeholder** drop-down to add changeable text fields to the subject line. When the alert is sent, the Service Portal populates the placeholder field with the relevant information.
  - c. **Text** – Edit the example contents of the Webhook alert. You can also use the **Placeholder** drop-down to add changeable text fields to the body content. When the alert is sent, the Service Portal populates the placeholder field with the relevant information.
  - d. **Alert to** – Use the check boxes to select which users you want to send the Webhook alert to:
    - **MSP Channels** – (Selected by default) All Channels created by MSP Admins receive the Webhook alert.
    - **Tenant Channels** – (Selected by default) All Channels created by Tenant Admins receive the Webhook alert.

6. When you're happy with your settings, click **Save**.

**Note:** You can edit  or delete  Service Levels from the Service Policy table.

### *Globally Disable Webhook Alerts*

By default, Webhook Alerts are enabled. Disabling Webhook alerts hides the Webhook tab from **System > General Settings** and the Webhook tab from the Tenant details area. Webhook Alert configuration is still visible when you

create a Service Level to enable configuration, but Webhook Alerts will not be sent while it is globally disabled.

1. From the main toolbar of the Service Portal, click **System > Policy and Reporting**, then select the **Policy** tab.
2. From the **Webhook Alerts** drop-down select **Disabled**.

## Scheduled Reporting

**Note:** Only MSP Administrators can configure scheduled reports.

You can configure the Service Portal to send out reports on a regular basis which summarize all the mitigated attacks in a set time period. The reports are created as PDFs and can be sent out to portal user's registered email addresses.

There are two types of report you can create:

- **Service Overview** – A report covering the attack information for your entire protected network, for the selected time period. This report can only be emailed to MSP Administrators and MSP Users.
- **Per-Tenant** – A report covering a single tenant's attack information, for the selected time period. This report can be emailed to MSP Administrators, MSP Users, Tenant Administrators, and Tenant Users.

### Report emails

When you set up a report you configure options to decide when the report email is sent and what information the email contains. To schedule the email, you select a time of day, in a specific timezone, to send the report. You can also select how often this report should be created and emailed.

**Note:** User's individual timezones do not affect when they receive reports. All reports are sent at the same time based on the report's timezone setting.

To accompany the report you can define an email subject and body containing further information about the attached report. You can include the following placeholders that the Service Portal will populate with information when it generates the email:

- **{report\_name}** – The name of this report as entered in the Name field (e.g. Weekly Report).
- **{report\_type}** – Whether this is a Service Overview or Per-Tenant report.
- **{report\_time\_period}** – Whether this report covers a span of a day, week, or month (e.g. day). If the report covers multiple days, weeks or months you should add an "s" after the placeholder.
- **{report\_time\_duration}** – The number of days, weeks or months covered in this report (e.g. 5).
- **{report\_start\_time}** – The time and date of the beginning of the reporting period (e.g. 11 Feb 2020 23:00 UTC+09:00).
- **{report\_end\_time}** – The time and date of the end of the reporting period (e.g. 12 Feb 2020 23:00 UTC+09:00).
- **{report\_generation\_time}** – The time and date this report was generated by the Service Portal (e.g. 13 Feb 2020 01:00 UTC+09:00).
- **{report\_time\_zone}** – The number of hours offset from UTC for the report's timezone (e.g. +09:00). You may wish to type UTC before the placeholder.

- **{tenant\_name}** – (Per-Tenant reports only) The name of the tenant (as it's written in their [Tenant Details](#)) who this report is about.

*Example: Service Overview report email*

Subject:

DDoS Service Overview Report

Body:

The attached service overview report provides information on all mitigated DDoS attacks between **{report\_start\_time}** and **{report\_end\_time}** (**{report\_time\_zone}**).

*Example: Per-Tenant report email*

Subject:

DDoS Service Report for **{tenant\_name}**

Body:

The attached report covers all mitigated DDoS attacks for **{tenant\_name}** over the past **{report\_time\_duration}** **{report\_time\_period}**s.

You can view more information about these attacks on the service portal Attack Analysis screen. Set the time frame between **{report\_start\_time}** and **{report\_end\_time}** (**{report\_time\_zone}**) to see the same results, or search for a specific attack using the Attack ID shown in the report.

## Scheduled Reporting screen

You can navigate to the Scheduled Reporting screen by clicking **System** on the main toolbar then the **Reporting** tab.

## Scheduled Reporting

[Add Report](#)

### Service Overview Reports

### Per-Tenant Reports

Name	Status	Send to	Report Type	Send every	Time	Actions
Daily report	● Active		Service Overview	1 Day	00:00:00	<a href="#">▶</a> <a href="#">✎</a> <a href="#">🗑</a>

◀ 1 ▶ 1 - 1 of 1 results

Show 5 ▼

There are two reports tables: **Service Overview Reports** and **Per-Tenant Reports**.

Each table contains the following information for each report:

- **Name** – Displays the name of this report.
- **Status** – Displays whether this report is currently **Active** or **Not active**. An activated report will be sent as scheduled but a deactivated report won't be.
- **Send to** – Displays the user roles who receive this report.
- **Report Type** – Displays whether this is a **Service Overview** report or a **Per-Tenant** report.
- **Send every** – Displays how often the report is generated and sent.
- **Time** – Displays the time of day the report is generated and sent.
- ▶/■ – Activate/deactivate the selected report.
- ✎ – Edit the selected report.
- 🗑 – Delete the selected report.

## Managing Scheduled Reporting

**Note:** This feature is only available to MSP Admin users.

If you want the Service Portal to create and send attack summary reports, you can configure scheduled reporting in the system settings.

### To add a report

1. From the main toolbar of the Service Portal, click **System**, then select the **Reporting** tab.
2. Click **Add Report**.

3. On the **Report Setup** tab, complete the following fields:

- **Name** – Type a name for this report.
- **Type** – Select the type of report you want to create (by default the report tab you are on is selected), from the following options:
  - **Service Overview** – A report covering the attack information for your entire protected network, for the selected time period.
  - **Per-Tenant** – A report covering a single tenant's attack information, for the selected time period.
- **Time Period** – Select the time period this report should cover. This covers full days from 00.00 to 23.59 in the selected report timezone.
- **Timezone** – From the drop-down, select the timezone for this report.
- **Repeat every** – Select how often the Service Portal should generate and send this report.
- **Runs at** – Select the time of day, in the selected report timezone, when the Service Portal should generate and send this report.



4. On the **Mail setup** tab, complete the following fields:

- **Subject** – Edit the example subject line for the report email.
- **Body** – Edit the example contents of the report email. Select a section of the text and use the **B**, **I**, and **U** buttons to add formatting. You can also use the **Placeholder** drop-down to add changeable text fields to the subject line. When the email is sent, the Service Portal populates the placeholder field with the relevant information. You can click **Send me a test report** to view how the email will look and see a dummy PDF report.
- **Send to** – Select the user roles you want to send this report to.
  - For Service Overview reports, you can only select from **MSP Admins** and **MSP Users** because the report covers all tenants.
  - For Per-Tenant reports, a different report is created for each tenancy and only the relevant report is sent to the Tenant Admins and Tenant User. You can select from **MSP Admins**, **MSP Users**, **Tenant Admins** and **Tenant Users**.

5. When you're happy with your settings, click **Save**.

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

#### *To activate/deactivate a report*

1. From the main toolbar of the Service Portal, click **System**, then select the **Reporting** tab.
2. From the table, find the report you want to enable or disable, and click  /  the activate/deactivate button.



## Usage Statistics

You can see how you're using the Service Portal in the Usage Statistics table. Every day the system checks how many tenants are enabled, how many assets have been assigned to all tenants, how many assets have been named, and how many tenant users there are.

You can use the **Export** button to download a .csv file of the data currently shown in the table.

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

### Usage Statistics screen

You can navigate to the Usage Statistics screen by clicking **System** on the main toolbar then the **Usage** tab.

Timescale: 24 Hours ▼
Export

USAGE STATISTICS				
Date/Time	Tenants	Tenant Assigned Assets	Tenant Named Assets	Tenant Users
2022-06-24 01:00	25	222	2000	0

◀ 1 ▶ 1 - 1 of 1 results
Show 5 ▼

You can use the **Timescale** filter drop-down to view usage from a preset or custom time period:

- 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.

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:

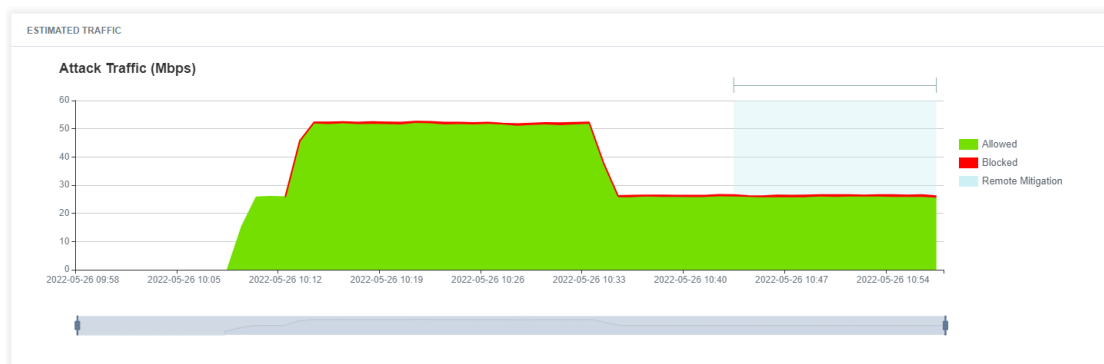
- Date/Time** – When the statistics were gathered
- Tenants** – The number of tenants enabled on the system

- **Tenant Assigned Assets** – The number of assets assigned to all tenants
- **Tenant Named Assets** – The number of assets which have been named by users
- **Tenant Users** – The total number of Tenant Administrators and Tenant Users in the Service Portal

## Remote Mitigation

**Note:** Only MSP Administrators can configure Remote Mitigation.

If your tenant's traffic is subject to an upstream Remote Mitigation (e.g. blackholed or rate limited), they will see their traffic rate reduce on the Service Portal. You can choose to show Remote Mitigations on traffic charts to inform your users and/or tenants about the reason their traffic rate has changed.



**Caution:** Only Remote Mitigations managed by the SmartWall CMS can be displayed on the Service Portal traffic charts. Any traffic management performed by a third-party product will not be shown as a Remote Mitigation on the Service Portal.

The CMS can be configured to send BGP and FlowSpec mitigations to your upstream router. BGP/FlowSpec routes are defined on the CMS using Route Templates. Route Templates describe the path you want traffic to follow when a Route is announced, and there should be a Route Template for each traffic handling method you require for your routing plan.

**Caution:** You must be actively using BGP and FlowSpec routes to handle traffic and your routes must be created using Route Templates. If you create a FlowSpec route using a FlowSpec Action, rather than a Route Template, you will not be able to see the Remote Mitigation in the Service Portal.

In the Service Portal, you can choose which of your Route Templates (e.g. which of your traffic handling methods) are shown on the Service Portal traffic charts as Remote Mitigations. You can also decide which of these Route Templates are shown to Tenants, as well as your MSP Users/Admin users. Any Route Templates which are used on the CMS, but are not added to the Remote Mitigations table on the Service Portal, will not appear on Service Portal traffic charts.



## Remote Mitigations screen

You can navigate to the Remote Mitigation screen by clicking **System > Policy and Reporting** on the main toolbar then the **Remote Mitigation** tab.

Remote Mitigation Display
Disabled



REMOTE MITIGATIONS

Add Remote Mitigation

Display Name	Description	Show For Tenants	Route Templates	Actions
Blackhole		False	Blackhole_1	 

1
1 - 1 of 1 results
Show
5

The Remote Mitigations table contains the following information for each report:

- **Display Name** – Displays the name of this Remote Mitigation. This is the name which will be displayed on the traffic charts.
- **Description** – Displays a description of this Remote Mitigation.
- **Show for Tenants** – Displays whether this Remote Mitigation will appear on the affected Tenant's traffic charts when active. If you have chosen not to show for tenants, this Remote Mitigation will only show on traffic charts for MSP User/Admin users.
- **Route Templates** – Displays the name of the Route Templates covered by this Remote Mitigation.
-  – Edit the selected report.
-  – Delete the selected report.

## Manage which Remote Mitigations are shown on the Service Portal

### Prerequisites

You must perform the following actions on the CMS:

- Your CMS configured as a BGP Client.
- You need a Route Template on the CMS for each traffic handling method you use for BGP/FlowSpec Mitigation on the CMS.
- You actively use the CMS to send BGP/FlowSpec routes to your upstream server.

### *To enable Remote Mitigation display in traffic charts*

By default, Remote Mitigation isn't shown on traffic charts.

1. From the main toolbar of the Service Portal, click **System > Policy and Reporting**.
2. Open the **Remote Mitigation** tab.
3. From the **Remote Mitigation Display** drop-down, select **Enabled**.

### *To manage which Remote Mitigations appear on traffic charts*

1. From the main toolbar of the Service Portal, click **System > Policy and Reporting**.
2. Open the **Remote Mitigation** tab.
3. Click **Add Remote Mitigation**.
4. Type a **Name** for this Remote Mitigation. This is the name which will be displayed on the traffic charts (E.g. Blackholed or Rate Limited).
5. (Optional) Type a **Description** for this Remote Mitigation.
6. Use the **Show For Tenant** box to choose whether this Remote Mitigation will appear on tenants traffic charts. If you have chosen not to show for tenants, this Remote Mitigation will only show on traffic charts for MSP User/Admin users.
7. Select all the Route Templates you want to be displayed with this Remote Mitigation name:
  - a. Click **Add Route Template**.
  - b. Type the name of the **Template**. This must exactly match the name of the Route Template stored in the CMS.
  - c. Repeat until you have all the Route Templates you require in the list.
8. Click **Save**.
9. Repeat steps 3-8 for every Remote Mitigation type that you want to be displayed with a different name.

## Notification Settings

**Note:** Webhook and email alert notifications are only available to MSP Admin and Tenant Admin users when enabled by an MSP Admin on the **System > Policy and Reporting > Policy** tab. Disabling either notification type for a Service Level will prevent any notifications from being sent.



The Service Portal can send alerts about attacks, traffic rates going above a tenant's Service Level, Remote Mitigation events and system health. These alert notifications can be sent to email recipients and Slack/Microsoft Teams channels. To do this, you must configure at least one notification for each desired alert type in the Service Portal. MSP Administrators can add notifications for the Service Portal as a whole, while Tenant Administrators can add notifications for alerts specific to their tenancy.



**Note:** Attack, Service Level and Remote Mitigation alert notifications are automatically sent by email to users based on their [Service Level](#) and user account preferences. The notifications you create in the Notifications tab allow alert messages to be sent to destinations without an associated user account. In the case of system health alerts, notifications can only be sent when configured from this tab, regardless of the destination.


Notification settings are accessed from the Notifications tab. You can access this from the main toolbar by clicking **System > Policy and Reporting > Notifications**. The Notifications tab contains the Webhooks panel and Email Addresses panel, where you can enter details of the alert notifications you wish to create.



**Note:** MSP Admin users can also edit the notification settings for a specific tenant from the Tenant Management screen after selecting a tenant in the left-hand pane.

## Webhooks screen

WEBHOOKS									
Name	Type	Webhook URL	Admin State	Service Lev...	Attack Statu...	Remote Miti...	System Heal...	Actions	
SlackNoteGeneral	Slack	https://hooks.sla...	Enabled	Enabled	Enabled	Enabled	Enabled	 	


1

1 - 1 of 1 results

Show
5


To add a new Webhook notification, click **Add Webhook**. You can also click the  **Edit Webhook** and  **Delete Webhook** icons in the **Actions** column to amend or remove an existing notification.

When adding or amending Webhook notifications, the following data fields will be displayed. Fields marked with an asterisk (\*) are required fields.

- **Name** — Type a **Name** for this Webhook.
- **Webhook URL** — Type the URL of your Slack/Teams incoming webhook URL.
- **Type** — From the **Type** drop-down, select if the Webhook is for **Slack** or **Microsoft Teams**.
- **Send Attack Alerts** — Select this check box to send attack alert notifications to this channel.
- **Send Service Level Alerts** — Select this check box to send service level alert notifications to this channel.
- **Send Remote Mitigation Alerts** — Select this check box to send Remote Mitigation alert notifications to this channel.
- **Send System Health Alerts** — Select this check box to send system health alert notifications to this channel.
- **Admin State** — By default, new alert notifications are enabled on creation, but you can change the **Admin State** to **Disabled** if you don't want to enable it now.
- **Send Test Message** — Test your configuration is correct by clicking this link to send a test message to your selected channel.





When you're happy with your configuration, click **Save**.



### Disabling All Webhook Alerts

By default, Webhook alert notifications are enabled. Disabling Webhook notifications hides the Webhook panel from the Notifications tab in both the Policy and Reporting screen and the Tenant Management screen. Alert types can still be enabled (or disabled) when you create or amend a Service Level, but Webhook alert notifications will not be sent while they are globally disabled.



1. From the main toolbar of the Service Portal, click **System > Policy and Reporting**, then select the **Policy** tab.
2. From the **Webhook Alerts** drop-down select **Disabled**.

## Email Addresses screen

EMAIL ADDRESSES										
Name	Address	Admin State	Service Level Al...	Attack Status Ale...	Remote Mitigatio...	Service Over...	Per-Tenant R...	System Health Al...	Admin Level	Actions
Domain Broadcast	dbroadcast@mon...	Enabled	Disabled	Disabled	Enabled	Disabled	Enabled	Enabled	Yes	 
Support John	jsupport@it.com	Enabled	Disabled	Enabled	Disabled	Disabled	Enabled	Enabled	No	 

 1  1 - 2 of 2 results

Show

To add a new email notification, click **Add Address**. You can also click the  **Edit Email Notification** and  **Delete Email Notification** icons in the **Actions** column to amend or remove an existing notification.

When adding or amending email notifications, the following data fields will be displayed. Fields marked with an asterisk (\*) are required fields.

- **Name** — Type a **Name** for this email notification.
- **Address** — Type an email address which will be the recipient for the notification.
- **Admin State** — By default, new alert notifications are enabled on creation, but you can change the **Admin State** to **Disabled** if you don't want to enable it now.
- **Service Level Alerts** — Select this check box to send Service Level alert notifications to this address.
- **Attack Status Alerts** — Select this check box to send attack status alert notifications to this address.
- **Remote Mitigation Alerts** — Select this check box to send Remote Mitigation alert notifications to this address.
- **Service Overview Reports** — Select this check box to send Service Overview report notifications to this address.
- **Per-Tenant Reports** — Select this check box to send Per-Tenant report notifications to this address.
- **System Health Alerts** — Select this check box to send system health alert notifications to this address.
- **Admin Level** — Use this drop-down to select whether the email address receives Administrator or User level notifications.

When you're happy with your configuration, click **Save**.



## Portal Management

The General Settings area provides administration options for the Service Portal.

### Licensing

**Note:** Only MSP Administrators can manage licenses.

When you install the Service Portal, you receive an evaluation license which allows you access to all of the Service Portal's features, but only allows you to create a maximum of 10 tenants.

**Note:** Earlier versions of the Service Portal allowed up to 25 tenants with an evaluation license. If you are upgrading from one of these versions, and you already created more than 10 tenants, no tenants will be deactivated. However, you will not be able to add any more until you acquire a full license.

When you're ready to upgrade to a full license, you need to contact your support representative, quoting your unique System UUID number. This is visible on the Licensing tab of the General Settings screen. Your support representative will then provide you with a license key that you need to enter on the Licensing tab to remove the evaluation tenant limit.

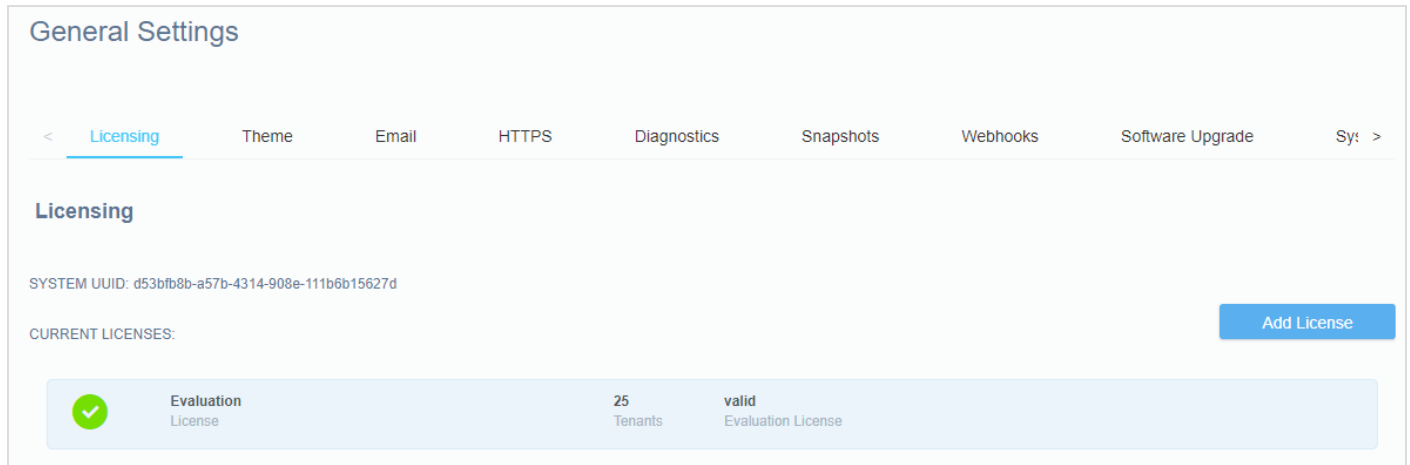
**Note:** The license is specific to your System UUID and cannot be used on any other Service Portal installation.

If your license has an expiry date, your support representative will make you aware of the following:

- The warning period – How long before the expiry date you will see expiry warnings in the Service Portal
- The grace period – How long after the license expires before the Service Portal is no longer accessible.

**Note:** If your Service Portal is connected to a TDD system, you can see your Juniper SSRN number displayed with your current license information.

You can navigate to the Licensing tab by clicking **System > General Settings > Licensing** on the main toolbar.



The Licensing tab displays information about your license as follows:

**SYSTEM UUID** – The unique number associated with your Service Portal installation.

**CURRENT LICENSES** – Details of your currently installed licence, including the license type, number of allowed tenants and the license status, which may be one of the following:

- Valid
- Expiring soon (showing expiry date)
- Expired (showing end of grace period date)
- Expired.

## Adding a License to the Service Portal

### *Prerequisites*

You must have a valid license key provided by your support representative.

### *To add a license to the Service Portal*

1. Copy the license key text to your clipboard.
2. From the main toolbar of the Service Portal, click **System > General Settings > Licensing**.
3. Click **Add License**.
4. In the field which appears, paste in the entire contents of the **License Key** text file, including the BEGIN and END header and footer lines.

Add License

Paste the license text in the form below.  
(The text must include the BEGIN and END header and footer lines)

```

-----BEGIN-CORERO-LICENSE-----
VeiJ3Z/2FTOfjsfXhTr65r7C9M4LIGTFwEBacssXnpbz0lvrrk2lO6XAbiLLjkua
XN/AQrmlP3lbPJCqtdkkk6eJvtdDxue/l/+8x3db4OKiyVQdHq5KjvpzKGmZjJL6
J9DU0xNmBR3Fq++hGNBtAg2QDRx9Lf9PhkBk4L4fhE2a1WvVjHlKK4FvBryWGz
G
BilGdnM6bHNr/ySzLU9Vmjppe9Q7MKkfh4ChGBN/+A7+Tz1h/e7yaAB9aGYC/0m
KyyIqXhQUamb6wIxRhJG7WoTp2ODIOZ8MFA51Zklq3GW8dGhrd6Stk/EQRMn2t
Z
EAM7MfNp69ccE7HaYwt1l2ingJFBfLnVb66sHxxefP6zpGrj8Q25N5QUuzbzQdZ
XkTdQZTRmY2cnQMIZU3Kg2aBA9fLAfGWAXzVvk416Tltdnlwr9bBEuNYGJc7peBEI
-----END-CORERO-LICENSE-----

```

Cancel
Save

- Click **Save**. The License tab will then update to show the new license details.

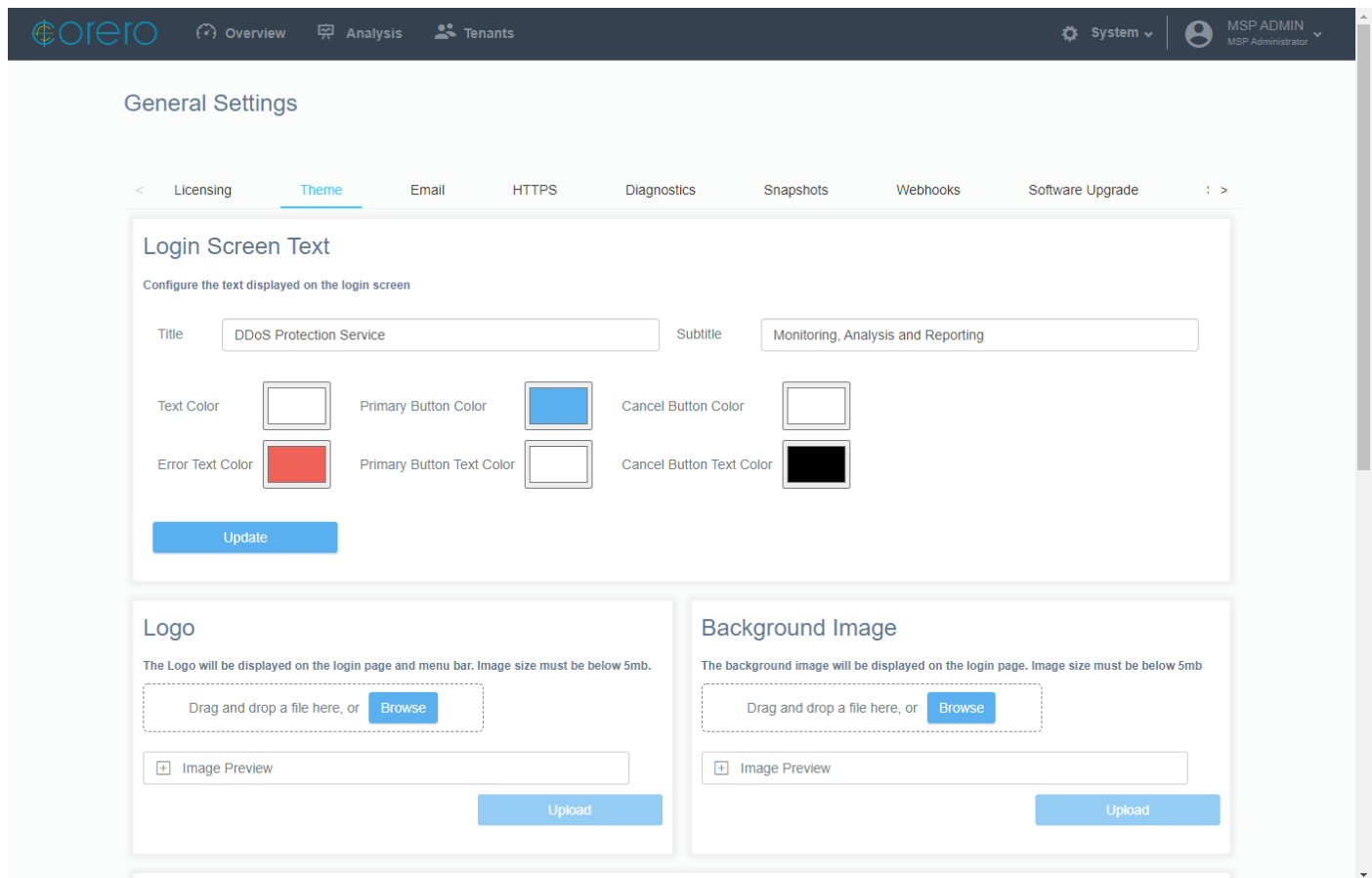
## Theme

**Note:** Only MSP Administrators can customize the theme settings.

Before you start adding tenants to the SmartWall Service Portal you should make sure the portal is branded for your organization. You can customize the login screen to better compliment your brand. You can also add a company logo that appears on the login screen, on the top left of the main toolbar, and on any reports generated by the Service Portal. When clicked the logo on the main toolbar acts as a home button, returning you to the Service Overview screen.

### Theme Settings Screen

You can navigate to the Logo tab of the System Settings Screen by clicking **System > General Settings** on the main toolbar, then the **Theme** tab.



The screenshot displays the Corero Service Portal interface. At the top, the navigation bar includes the Corero logo, 'Overview', 'Analysis', 'Tenants', 'System', and a user profile for 'MSP ADMIN'. The 'System' dropdown is open, showing 'General Settings'. The 'General Settings' page has several tabs: 'Licensing', 'Theme' (selected), 'Email', 'HTTPS', 'Diagnostics', 'Snapshots', 'Webhooks', and 'Software Upgrade'. The 'Theme' tab contains three main sections:

- Login Screen Text:** A section for configuring the text on the login screen. It includes input fields for 'Title' (DDoS Protection Service) and 'Subtitle' (Monitoring, Analysis and Reporting). Below these are color pickers for 'Text Color', 'Primary Button Color', 'Cancel Button Color', 'Error Text Color', 'Primary Button Text Color', and 'Cancel Button Text Color'. An 'Update' button is at the bottom.
- Logo:** A section for uploading a logo. It includes a 'Browse' button, an 'Image Preview' field, and an 'Upload' button. A note states: 'The Logo will be displayed on the login page and menu bar. Image size must be below 5mb.'
- Background Image:** A section for uploading a background image. It includes a 'Browse' button, an 'Image Preview' field, and an 'Upload' button. A note states: 'The background image will be displayed on the login page. Image size must be below 5mb.'

You can customize the following features here:

- **Login Screen Text:**
  - **Title** – Edit the default title which appears on the login screen.
  - **Subtitle** – Edit the text that appears below the default title on the login screen.
  - **Text Color** – Change the text color used for all general text on the login screen. By default, this is white.
  - **Error Text Color** – Change the text color used for any error text shown on the login screen. By default, this is red.
  - **Button Color** – Change the color of the Log in button on the login screen. By default, this is light blue.
  - **Button Text Color** – Change the text color used on the Log in button on the login screen. By default, this is white.
- **Logo** – Upload an image of your company logo.
- **Background Image** – Upload a background image for the login screen.
- **Terms of Service** – Customize the text on the login screen that includes a hyperlink to your company's terms of service document.
- **Favicons** – Upload the image you want to appear on a browser tab, favorite bar or shortcuts.
- **Webpage Title** – Change the text that appears at the top of a browser tab which contains the portal.
- **Reset to Defaults** – Reset all Theme settings to the default Corero theme.

## Customizing the Service Portal Theme

**Note:** This feature is only available to MSP Admin users.

To provide a more familiar experience for your Tenants, you can customize the login screen your users see when they access the Service Portal to reflect your company branding.

Theme settings can be configured on **System > General Settings > Theme**. The image below shows how the configuration settings apply on the login screen.



*To customize the text shown on the login screen*

1. From the main toolbar of the Service Portal, click **System > General Settings**, then the **Theme** tab.
2. Navigate to the **Login Screen Text** area on the screen.

3. You can modify the following areas:

- **Title** – Edit the default title which appears on the login screen.
- **Subtitle** – Edit the text that appears below the default title on the login screen.
- **Text Color** – Change the text color used for all general text on the login screen. By default, this is white.
- **Error Text Color** – Change the text color used for any error text shown on the login screen. By default, this is red.
- **Primary Button Color** – Change the color of the Log in button on the login screen. By default, this is light blue.
- **Primary Button Text Color** – Change the text color used on the Log in button on the login screen. By default, this is white.
- **Cancel Button Color** – Change the color of the Cancel button on the password recovery and token screens. By default, this is white.
- **Cancel Button Text Color** – Change the text color used on the Cancel button on the password recovery and token screens. By default, this is black.

4. Click **Update**.

5. You can verify the final design by logging out of the Service Portal to view the log in page.

#### *To add your company logo to the Service Portal*

1. Prepare a logo image for upload and save locally. The image must adhere to the following criteria:
  - The file size must be less than 5 MB
  - The file format must be PNG or JPG
2. From the main toolbar of the Service Portal, click **System > General Settings**, then the **Theme** tab.
3. Navigate to the **Logo** area on the screen.
4. Either drag and drop an image onto the logo area, or click **Browse** to select an image file from your computer.
5. Once the logo has successfully uploaded you should see it appear on the top left of the main toolbar and on the log in page.

**Note:** This logo appears on the login screen, the main toolbar of the Service Portal, and on reports generated by the Service Portal.

#### *To change the background image on the login screen*

1. Prepare a background image for upload and save locally. The image must adhere to the following criteria:
  - The file size must be less than 5 MB
  - The file format must be PNG or JPG
2. From the main toolbar of the Service Portal, click **System > General Settings**, then the **Theme** tab.
3. Navigate to the **Background Image** area on the screen.
4. Either drag and drop an image onto the logo area, or click **Browse** to select an image file from your computer.

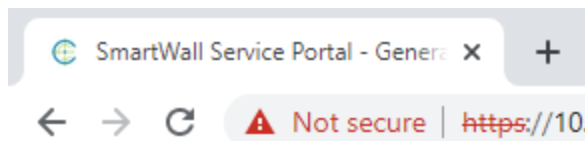
5. Once the image has successfully uploaded you can see a preview and verify the final design by logging out of the Service Portal to view the log in page.

#### *To customize the terms of service link at the bottom of the login screen*

1. From the main toolbar of the Service Portal, click **System > General Settings**, then the **Theme** tab.
2. Navigate to the **Terms of Service** area on the screen.
3. Type the **URL** to the site containing your terms of service document.
4. In the **Text** field, type the text you want to appear at the bottom of the login screen. The section of the text you want to use as a hyperlink must be encased in curly brackets. For example, the following text `By continuing, you agree to the {terms of service}.` would create a hyperlink on "terms of service" which would take the customer to the configured URL.
5. Click **Update**.
6. You can verify the final design by logging out of the Service Portal to view the log in page.

#### *To customize the browser tab*

You can change the image and title text which appears on a browser tab which has the Service Portal open. These settings will also customize how the Service Portal looks as a favorites bar option or shortcut.



1. From the main toolbar of the Service Portal, click **System > General Settings**, then the **Theme** tab.
2. To change the favicon image:
  - a. Prepare two favicon images for upload and save locally. The image must adhere to the following criteria:
    - One image must be 16px by 16px, the second image must be 32px by 32px.
    - The file format must be PNG
  - b. Navigate to the **Favicon** area on the screen.
  - c. Either drag and drop the images onto the correct favicon areas, or click **Browse** to select the image files from your computer.
  - d. Once the images have successfully uploaded you should see it appear in your browser tab.
3. To change the webpage title text:
  - a. Navigate to the **Webpage Title** area on the screen.
  - b. In the **Text** field, type the text you want to appear as the title in the browser tab.
  - c. Click **Update**. You should see the new text appear in your browser tab.



### To reset the theme to default

If you need to return the Service Portal to the default theme settings (as shown in image above), you can remove all changes.

1. From the main toolbar of the Service Portal, click **System > General Settings**, then the **Theme** tab.
2. Navigate to the **Reset to Defaults** area on the screen and click **Reset**.
3. Click **OK** to confirm.

## Email Settings

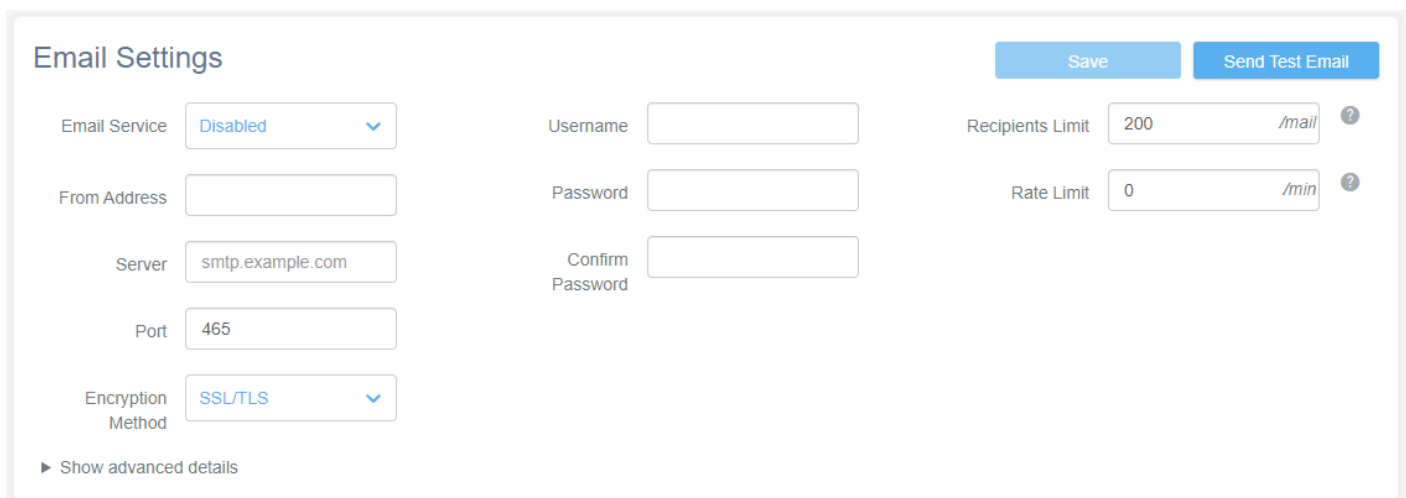
**Note:** Only MSP Administrators can configure email settings.

The SmartWall Service Portal has multiple features which rely on the ability to send emails to users (i.e. sending service level and attack alerts, sending scheduled reports, and password recovery). To enable the Service Portal to send emails, you must configure a mail server.

Additionally, the Service Portal stores a record of all emails sent enabling you to review email history.

### Email Settings screen

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



The screenshot shows the 'Email Settings' configuration page. At the top right are 'Save' and 'Send Test Email' buttons. The settings are organized into three columns:

- Left Column:**
  - Email Service: Disabled (dropdown)
  - From Address: (text input)
  - Server: smtp.example.com (text input)
  - Port: 465 (text input)
  - Encryption Method: SSL/TLS (dropdown)
- Middle Column:**
  - Username: (text input)
  - Password: (text input)
  - Confirm Password: (text input)
- Right Column:**
  - Recipients Limit: 200 /mail (text input with help icon)
  - Rate Limit: 0 /min (text input with help icon)

At the bottom left, there is a link 'Show advanced details'.

### Configuring a mail server

You must configure a mail server on your Service Portal to enable it to send emails to users for password recovery, alerts, and reporting.

### *To configure your mail server*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Email** tab.
3. From the **Email Service** drop-down, select **enabled** to enable sending emails.
4. Enter the required information about your mail server:
  - **From Address** – Type the email address you want to appear as the sender on all emails sent from the Service Portal.
  - **Server** – Type your server address (e.g. smtp.example.com).
  - **Port** – Type your mail port on the server (default: 465).
  - **Username** – Type a username for your mail server with the necessary credentials to send emails.
  - **Password** and **Confirm Password** – Type the password associated with that username in both password fields.
  - **Recipients List** – The maximum number of recipients allowed per mail, inclusive of TO, CC and BCC (default: 200). To have no limit on recipient numbers enter 0.
  - **Rate Limit** – The maximum number of emails sent per minute (default: 0). To have no limit the number of emails sent per minute enter 0.
  - **Encryption Method** – From the drop-down, select your encryption method: **None**, **SSL/TTS**, or **STARTTLS** (default: SSL/TTS).
5. To test your configuration by sending an email to your own email address, click **Send Test Email**.
6. Click **Save**.

### *To configure timeout periods*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Email** tab.
3. In the Email Settings area, click **Show advanced details**.
4. Configure any of the following timeout fields:
  - **Connection Timeout** – Type a socket connection timeout in milliseconds (default: 5000). If you don't want a timeout, type 0.
  - **Timeout** – Type a socket I/O read timeout in milliseconds (default: 10000). If you don't want a timeout, type 0.
  - **Write Timeout** – Type a socket I/O write timeout in milliseconds (default: 10000). If you don't want a timeout, type 0.
  - **Max Email Age** – Type the maximum number of days an email is recorded for (default: 730 days).
5. To test your configuration by sending an email to your own email address, click **Send Test Email**.
6. Click **Save**.

## Managing email history

The Email History panel contains a log of all emails sent by the Service Portal enabling you to review what has been sent, identify any errors, and export information.

### *To view email history*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Email** tab.
3. In the Email History panel, you can view a list of the most recent sent emails. You can filter this list in the following ways:
  - **Search** – Identify emails containing keywords in the following areas:
    - **Type** – Show all email log entries of the type entered in the search bar.
    - **Subject** – Show all email log entries containing the keywords entered in the search bar in the subject of the email.
    - **Recipient** – Show all email log entries for a recipient name/email address entered in the search bar.
    - **Delivery Status** – Show all email log entries of the status type entered in the search bar.
  - **Timescale** – Filter the table to show results from any of the following time periods:
    - **Last Hour** – Only data from the last hour (Default)
    - **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.


### *To export email history*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Email** tab.
3. Filter the Email History table to show the results you want to export.
4. Click **Export Selection to CSV**.
5. A .csv file will now download in your browser.

### *To clear email history*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Email** tab.
3. In the Email History panel, click **Clear History**.
4. Click **Yes**.

### To view email history log entry details

You can examine the details for each entry in the Email History panel by clicking the  Information icon in the Actions column. This will display a detailed log of all the actions performed in connection with a single email send operation. If any errors are encountered, the information on this screen will allow you to diagnose the problem. SMTP error codes and explanatory text are included in the Error column to aid resolution.

In the example below, SMTP error 550 indicates that an invalid address was used in specifying the message recipient.

#### Email History

Type	System Health Notification
Created Time	2022-10-27 13:47
Last Updated Time	2022-10-27 13:49
Subject	System health alert Raised: System - pm-tds-swa.corero.com - CMS Portal Integration disabled
Recipient	test@test.com
Status	Expired
Error	Too many failed attempts
Attachment Included	false
Description	System Health Alert

#### HISTORY

Date/Time	Status	Error
2022-10-27 13:51	Queued	
2022-10-27 13:51	Retry	SMTP error code 550 received with message [550 Invalid sender noreply@te:
2022-10-27 13:51	Retry	SMTP error code 550 received with message [550 Invalid sender noreply@te:
2022-10-27 13:51	Expired	Too many failed attempts

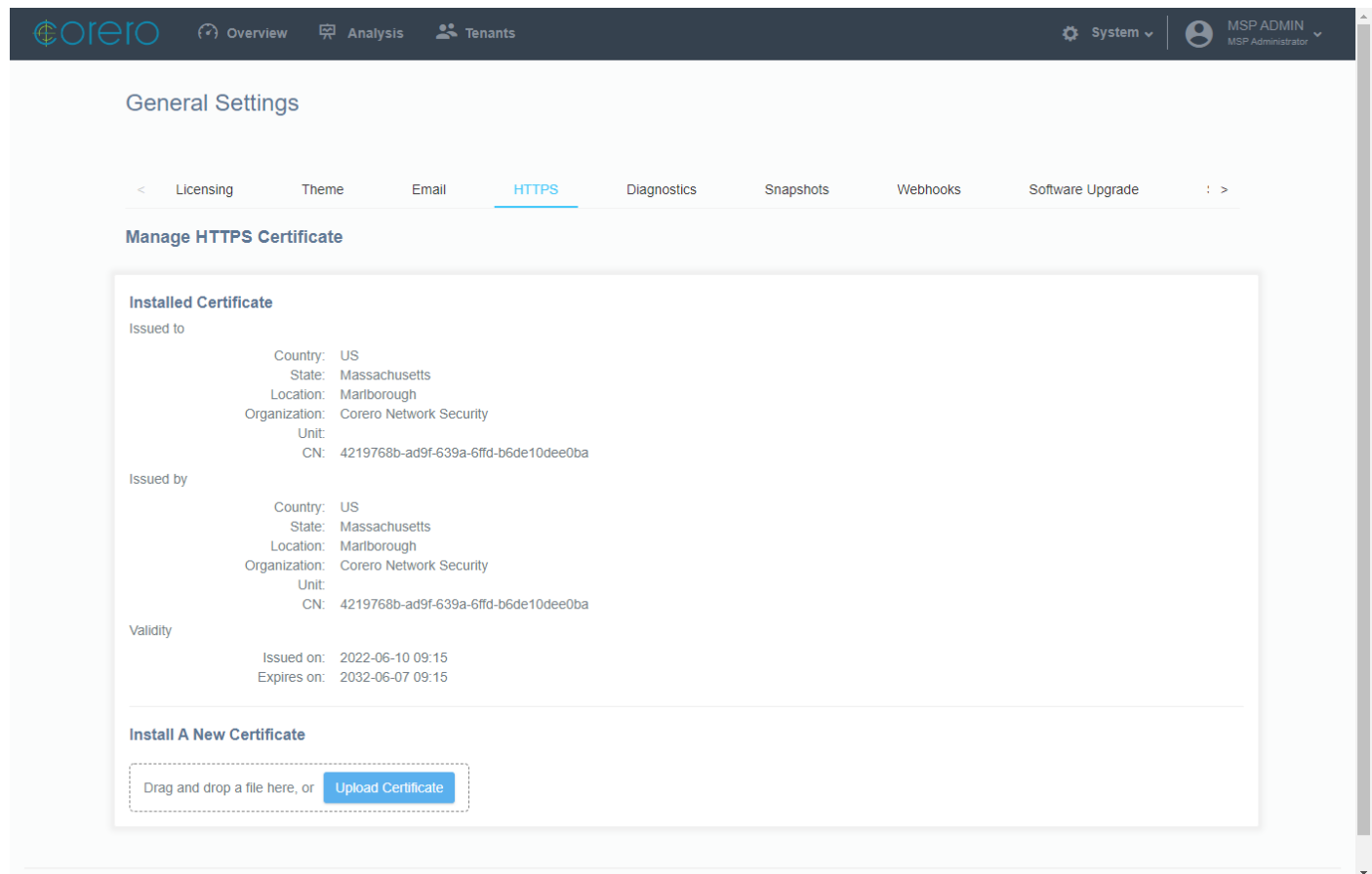
## HTTPS

**Note:** Only MSP Administrators can configure HTTPS settings.

The Service Portal comes with a default self-signed Corero SSL certificate which your browser will list as "not secure". As soon as possible, you should replace this with a signed certificate.

### HTTPS screen

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



### Add a signed certificate to the Service Portal

You can upload a signed SSL certificate to the Service Portal

**Note:** Certificates must be packaged in pkcs12 format and can optionally be password protected. The pkcs file should contain a single private key and certificate pair.

*To upload a signed certificate*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **HTTPS** tab.
3. Click **Upload Certificate**.
4. Select a pkcs12 certificate file on your computer, and click **Open**.
5. (Optional) Type in the **Password** for the certificate file.
6. Click **OK**.
7. If necessary, refresh the browser to ensure the new certificate has been loaded.

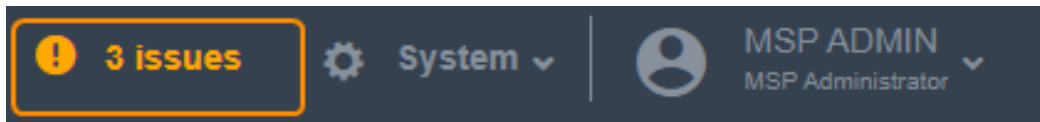
## Portal Health Monitoring

**Note:** Only MSP Administrators can view health alerts.

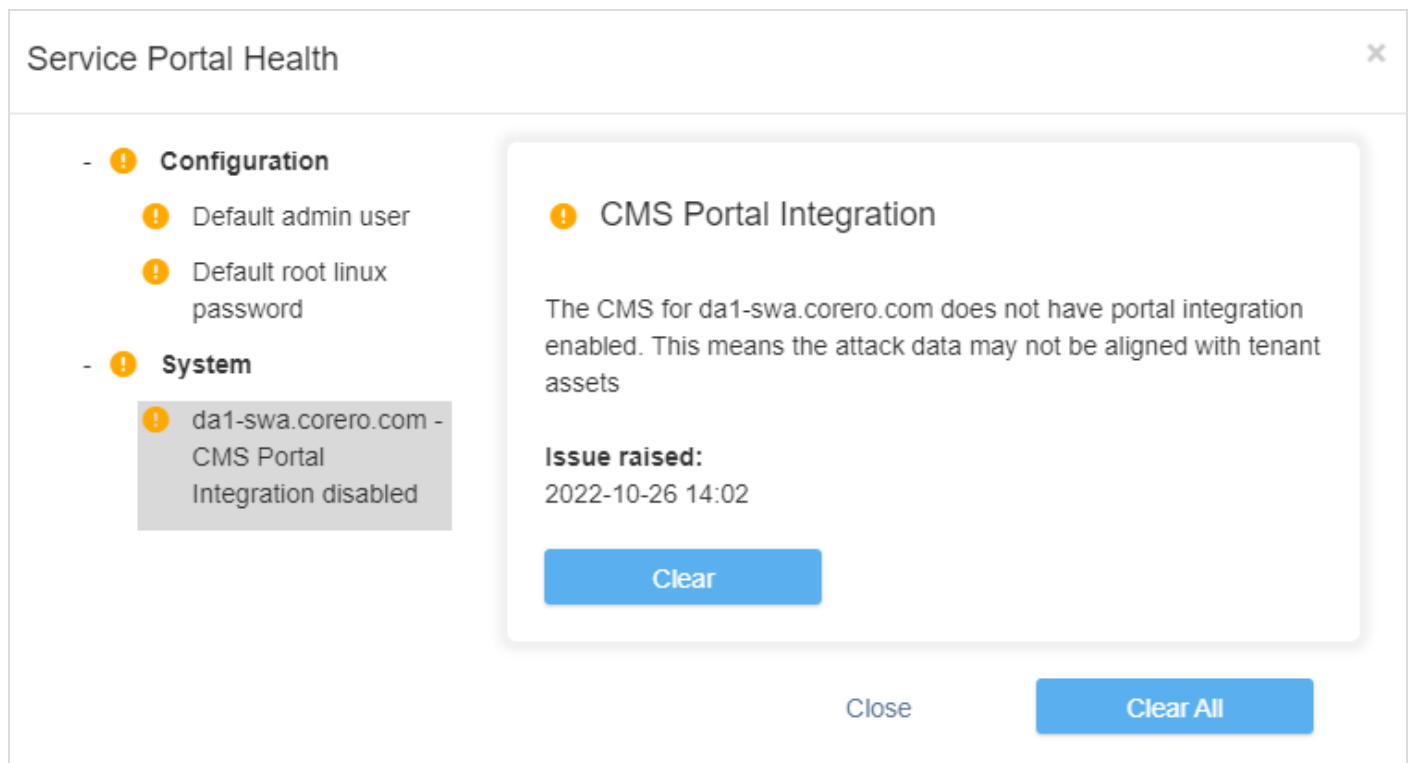
The Service Portal actively monitors itself for potential issues, and will generate a health alert whenever it detects an issue which may affect the security or correct operation of the system

### Viewing alerts

Any detected issues will cause a yellow icon to appear on the main toolbar, together with a text display of the number of issues detected.



Clicking on the icon will display the **Service Portal Health** screen, which displays health alerts categorized as type **Configuration**, **Portal Feed** or **System**.



Clicking on the alert notification listed in the left pane will display a description of the detected issue in the right pane. You can click on **Clear** after selecting an alert to remove it from the Service Portal Health screen, or click **Clear All** to remove all displayed alerts. However, unless you take action to address the underlying issue, the alert will re-

appear when the system health is re-checked. Some alerts will automatically be cleared if the underlying issue is resolved. You can access a history of all health alerts logged for a given time period in the System Health Log tab on the [Diagnostics screen](#).

## Health alert types

The following health alerts may be generated:

### Configuration alerts

<b>Alert name</b>	Default admin user
<b>Severity</b>	Warning
<b>Description</b>	The default MSP Administrator account created during installation still exists. This represents a security risk.
<b>Monitoring</b>	The issue is checked for on application start, when the system time reaches 00:00 (midnight), and each time an account is deleted.
<b>Resolution</b>	Automatically cleared when the default account is deleted.

<b>Alert name</b>	Default root linux password
<b>Severity</b>	Warning
<b>Description</b>	The default root login password for the Service Portal host's operating system created during installation is still active. This represents a security risk.
<b>Monitoring</b>	The issue is checked for on application start, and every 5 minutes thereafter.
<b>Resolution</b>	Cleared automatically when the default root password is changed.

### Portal feed alerts

<b>Alert name</b>	No syslog
<b>Severity</b>	Warning
<b>Description</b>	No syslog messages have been received from the referenced SWA host in the last 1 minute.



<b>Monitoring</b>	The issue is checked for on application start, every 1 minute thereafter and whenever a SWA host is decommissioned (deleted from the SWA Status tab on the <a href="#">Diagnostics screen</a> ).
<b>Resolution</b>	Cleared automatically if syslog messages resume from the referenced SWA host, or the SWA host is decommissioned.

### System alerts

<b>Alert name</b>	Unsupported version
<b>Severity</b>	Warning
<b>Description</b>	An unsupported version of a connected application for the indicated SWA host has been detected. The alert description will include both the unsupported and minimum supported versions to assist in determining the upgrade steps required.
<b>Monitoring</b>	The issue is checked for on application start, every 1 minute thereafter and whenever a SWA host is decommissioned.
<b>Resolution</b>	Cleared automatically if a new version of the connected application is detected, or the SWA host is decommissioned.

<b>Alert name</b>	CMS portal integration
<b>Severity</b>	Warning
<b>Description</b>	The CMS application connected to the indicated SWA host does not have portal integration enabled. This means that attack data may not be aligned with Tenant Assets.
<b>Monitoring</b>	The issue is checked for on application start, every 1 minute thereafter and whenever a SWA host is decommissioned.
<b>Resolution</b>	Cleared automatically when portal integration is enabled on the connected CMS, or the SWA host is decommissioned.

## Diagnostics

**Note:** Only MSP Administrators can access the diagnostic options.

The Service Portal contains a number of diagnostic options designed to help you identify and correct issues either with the application itself or with connected devices. These can be accessed via the Diagnostics page. The following tabs are available within the Diagnostics screen:

- System Health Log
- SWA Status
- Logger Configuration
- Aggregated DIP Traffic
- Diagnostic Dump

### Accessing the Diagnostic screen

You can navigate to the Diagnostic screen by clicking **System > Diagnostics** on the main toolbar.

### System Health Log

To access this tab, click **System Health Log** in the Diagnostics screen.

### System Health Log

Username

☒ Display system actions  
☒ Display cleared  
☒ Display raised

Export

Timescale:

Last Hour

Date/Time	User	Action	Category	Issue	Severity	Description
2022-10-24 08...	system	Raised	Portal Feed	da1-swa.corero.com -	Warning	No syslog messages have been received from da1-
2022-10-24 08...	system	Raised	System	da1-swa.corero.com -	Warning	The CMS for da1-swa.corero.com does not have po
2022-10-24 08...	system	Raised	System	da1-swa.corero.com -	Warning	The CMS for da1-swa.corero.com does not have po

< 1 >

1 - 3 of 3 results

Show

5


The System Health Log tab displays a list of all logged health alerts which describe detected health issues, using the currently selected display criteria, which you can set with the following controls:

- **Timescale** – You can select the time period for displayed alerts from the drop-down list
- **Username** – You can search for alerts related to a specific user by entering the required **Username** in the search box
- **Display system actions** – Use this check box to toggle the display of system-generated alerts
- **Display cleared** – Check this box to specify that alerts which have already been cleared within the specified time period will be included in the displayed list
- **Display raised** – Check this box to specify that all alerts raised within the specified time period will be included in the displayed list
- **Export** - Click this button to export the currently displayed list as a CSV file (`health-issue-change.log.csv`) which will be saved to your browser's currently configured download location.

The information displayed on this tab will also be included in the [Diagnostic Dump](#) when it is generated.

## SWA Status

To access this tab, click **SWA Status** in the Diagnostics screen.


SWA Host	SWA Version	Corero Alert Actions Version	Portal Feed Version	CMS Version	CMS IP Intelligence	CMS Service Portal Sync	SWA Service Portal Sync	Last Syslog Received	Actions
da1-swa.corer...	11.7.0.0026	11.5.0.0008	4.7.1.0001	11.5.1.0007	Disabled	Disabled	Enabled	2022-10-24 10...	

< 1 > 1 - 1 of 1 results
 Show

The SWA Status tab shows dynamic status details for all currently connected SWAs. The display is refreshed approximately once per minute. The details displayed include:

- **SWA Host** – The hostname of the connected SWA
- **SWA Version** – The SWA application software version
- **Corero Alert Actions Version** – The Corero Alert Actions application version installed on the SWA
- **Portal Feed Version** – The version of the Service Portal Feed application installed on the SWA
- **CMS Version** – The version of the CMS connected to the SWA
- **CMP IP Intelligence** – The version of the IP Intelligence plug-in (null if not installed)

- **CSM Service Portal Sync** – The status of the CMS sync to the Service Portal
- **SWA Service Portal Sync** – The status of the SWA sync to the Service Portal
- **Last Syslog Received** – The date/time the last syslog message was received

You can optionally remove a SWA from the list by clicking  the **Delete SWA** button, for example if you have intentionally powered down the SWA instance. However, if syslog messages are subsequently received from the deleted SWA, it will reappear in the SWA Status tab.

## Logger Configuration

To access this tab, click **Logger Configuration** in the Diagnostics screen.

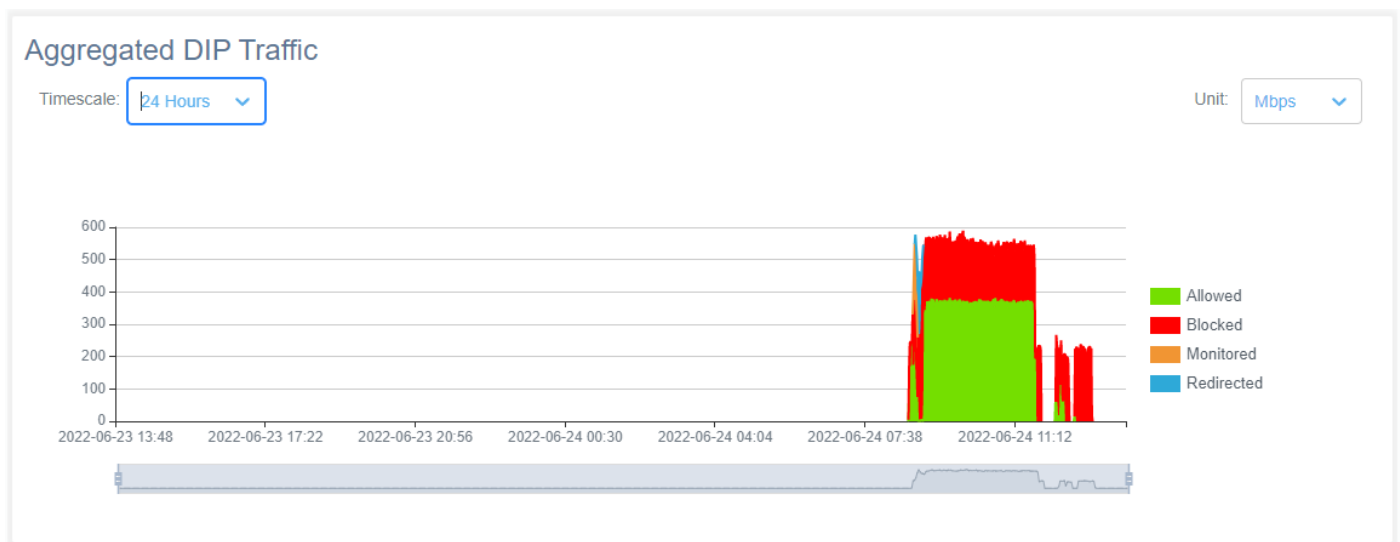
**Note:** This feature should only be used under the specific guidance of support staff.

The Logger Configuration tab allows you to set specific logging behavior for selected application components which underpin the operation of the the Service Portal. When you click **Add logger**, you will be prompted for a **Logger Name** (the name of the component) and a **Log Level** (the amount/type of detail to be logged). Note that only valid component names will be accepted.

The default **Log Level** for components will be `INFO` unless otherwise specified in this tab.

## Aggregated DIP Traffic

To access this tab, click **Aggregated DIP Traffic** in the Diagnostics screen.



The Aggregated DIP Traffic chart shows the rate of blocked and allowed traffic across your protected network in the selected time period. Unlike the traffic chart on the Service Overview screen which uses IP-based traffic samples, this

traffic chart shows the data from the Interface and Rule counters on the Defense devices and provides a layer 2 view. Differences between the two charts may help you identify any system issues.

You can use the **Timescale** filter drop-down to view traffic 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.

You can use the **Units** filter drop-down to change the chart between showing the traffic rate in **Mbps** (Megabits per second) or **PPS** (Packets per second).

## Diagnostic Dump

To access this tab, click **Diagnostic Dump** in the Diagnostics screen.

### Diagnostic Dump

☐ Database dump
 ☐ Include Traffic Data
 ☐ Anonymized Data

Request Diagnostic Dump

You can use this feature to assist Corero Customer Support or for your own investigations into an issue, by downloading a set of diagnostic files which can optionally contain the information from the Service Portal database. Data on actions, events, and other information which can be useful to review when trying to diagnose an issue with the Service Portal are included in the output. If Corero Customer Support asks for a diagnostics file, you can download either:

- The diagnostic files
- The diagnostic files and a database dump
- The diagnostic files and an anonymized database dump (where company and customer details are removed)

## To download Service Portal diagnostics

1. From the main toolbar of the Service Portal, click **System > Diagnostics**, then the **Diagnostic Dump** tab.
2. (Optional) Select **Database dump** to include the data stored on the Service Portal. You can then choose to modify the database dump in the following ways:
  - (Optional) Select **Include traffic data** to include the stored traffic information.
  - (Optional) Deselect **Anonymized Data** if you need to see specific customer or company information in that Database dump.
3. Click **Request Diagnostic Dump**. You will see the In Progress icon appear.
4. Once it has completed, click **Download**. The diagnostic package should now download using your browser.

## Snapshots

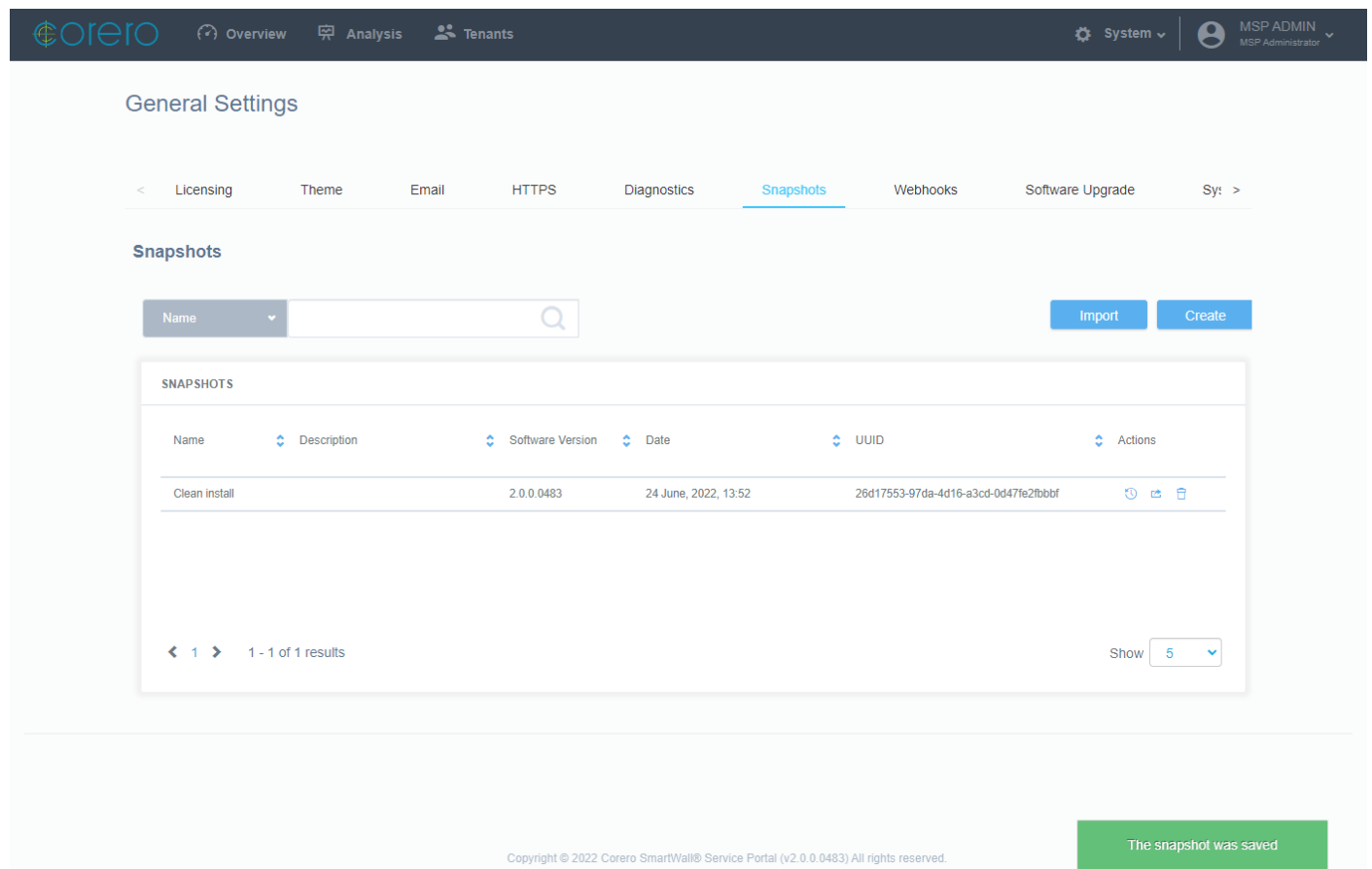
**Note:** Only MSP Administrators can manage snapshots.

A snapshot is a package file containing the configuration of the Service Portal at the moment you create it. You can create one at any time and store multiple snapshots in the Service Portal. You may want to take a snapshot before you make a large configuration change so you have the option to restore the previous settings.

If you choose to restore a snapshot, it deletes the current Service Portal configuration and replaces it with the saved copy. This excludes the snapshot list, which does not change. This enables you to move back and forth between snapshots.

### Snapshots screen

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



The screenshot shows the Corero Service Portal interface. The top navigation bar includes the Corero logo, tabs for Overview, Analysis, and Tenants, and a System dropdown menu. The user is logged in as MSP ADMIN. The main content area is titled 'General Settings' and contains a horizontal tab bar with options: Licensing, Theme, Email, HTTPS, Diagnostics, Snapshots (selected), Webhooks, Software Upgrade, and Sy. Below the tabs, the 'Snapshots' section features a search bar with a dropdown menu and buttons for 'Import' and 'Create'. A table titled 'SNAPSHOTS' displays the following data:

Name	Description	Software Version	Date	UUID	Actions
Clean install		2.0.0.0483	24 June, 2022, 13:52	26d17553-97da-4d16-a3cd-0d47fe2fbbf	⌚ ⌄ 🗑

At the bottom of the table, there is a pagination control showing '1 - 1 of 1 results' and a 'Show' dropdown set to '5'. A green notification banner at the bottom right states 'The snapshot was saved'. The footer contains the copyright notice: 'Copyright © 2022 Corero SmartWall® Service Portal (v2.0.0.0483) All rights reserved.'

## Manage Snapshots

Periodically, or before you perform a large configuration change, you may want to create a snapshot of the Service Portal's configuration.

**Caution:** Snapshots are version specific. After you upgrade the Service Portal, you will not be able to use any saved snapshots from the previous version. The snapshots remain available in the Service Portal after an upgrade to enable you to export them if needed.

### *To create a snapshot*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Snapshots** tab.
3. Click **Create**.
4. Type a **Name** for your new snapshot.


**Caution:** Snapshot names cannot contain any spaces. Only alphanumeric or .-&()\_: symbols.

5. (Optional) Type a **Description** of the snapshot.
6. Click **Save**.

**Tip:** On the Snapshots table, you can delete  snapshots you no longer need.

### *To restore configuration from a snapshot*

If you want to return to a previous configuration, you can restore an earlier snapshot. Restoring a snapshot does not erase your later snapshots, enabling you to move between snapshots to investigate configuration changes.

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Snapshots** tab.
3. From the table, locate the snapshot you want to restore and click  the restore button. You can type a text string into the Search field to narrow down the list.
4. Confirm snapshot restore, click **OK**.


**Caution:** Restoring a snapshot will cause the Service Portal to restart.

### *To export a snapshot*

You can import snapshots you have exported from other Service Portals or which you exported from this Service Portal application to store externally. If you choose to password protect a snapshot, you must provide this password when you import the snapshot.

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Snapshots** tab.



3. From the table, locate the snapshot you want to export and click  the export button. You can type a text string into the Search field to narrow down the list.
4. (Optional) If you want to password protect the snapshot, type in a **Password** and **Repeat Password**.
5. Click **Save**.
6. The snapshot package file is downloaded by your browser.

#### *To import a snapshot*

You can import snapshots you have exported from other Service Portals or which you exported from this Service Portal application to store externally. Once you import a snapshot you can view it in your snapshot list and use it like any other.

1. Use the left-hand menu to navigate to **System > Snapshots**.
2. Click **Import**.
3. Select the snapshot on your computer and click **Open**.
4. (Optional) If the snapshot is password protected, type in the **Password**.
5. Click **OK**.

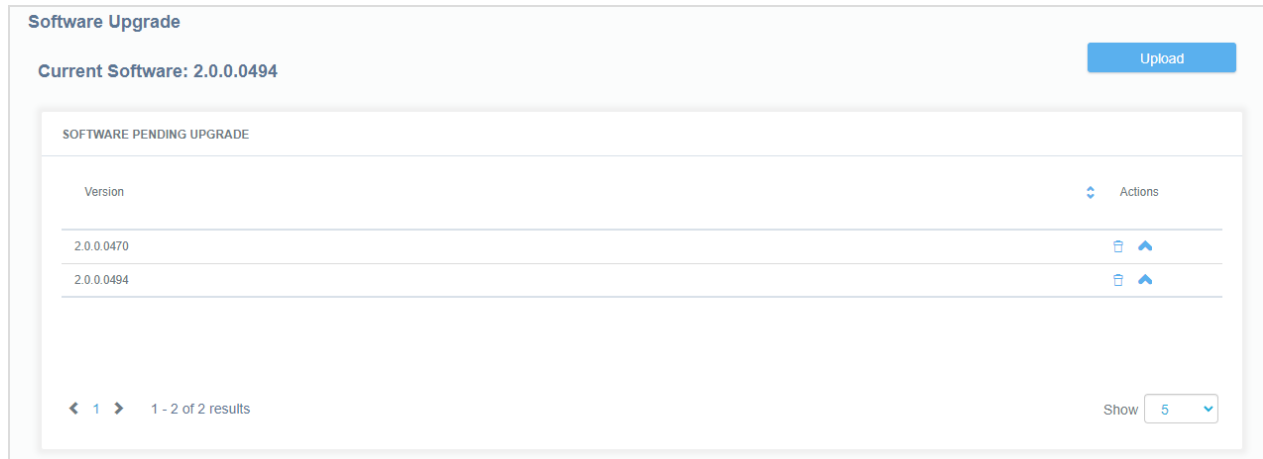
**Note:** If you restore a snapshot which was generated in a different Service Portal, you will not receive traffic history and the email/slack alerts will be disabled.

## Software Upgrade

### Upgrading the Service Portal application software

**Note:** Only MSP Administrators can perform software upgrades.

You can use the Software Upgrade tab to update your Service Portal application software. To access this feature, click **System > General Settings** on the main toolbar, then select the **Software Upgrade** tab. The current version of the software is displayed above the upgrade table.




### To update the Service Portal application software

#### Prerequisites

- You will receive an upgrade package file from your support representative. Save this file locally.
- (Optional) Take a snapshot of the Service Portal VM using a suitable management utility.

### To upgrade your Service Portal

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **Software Upgrade** tab.
3. Click **Upload**.
4. Select a Service Portal upgrade package file (.pkg) and click **Open**.
5. In the Software Pending Upgrade table, locate the version you want to upgrade the Service Portal to and click  the upgrade button.
6. The Service Portal will now perform pre-upgrade checks to make sure the upgrade file is compatible with your application version. If any of the checks fail, you will see a failure report and the upgrade will be aborted. If the checks all pass, you can continue to the next step.

**Note:** The failure report shown for unsuccessful pre-upgrade checks should inform you of any modifications required to complete the upgrade. You can make these changes and try the

upgrade again. If you are unable to resolve the issue and complete an upgrade, contact your support representative.

7. Once the pre-upgrade checks have completed successfully, you will be presented with a URL. Save a copy of this URL, as it contains a UUID which provides access to your upgrade progress screen. You will be automatically redirected there once the upgrade begins, but if you close the browser, you will need a copy of the URL to access this screen again.
8. Click **Upgrade**. You will be redirected to the upgrade progress screen while the application restarts.
9. Once the upgrade is complete, log back in to the Service Portal and check the software version number displayed at the top of the Home screen shows the expected version.

## Upgrading the Linux operating system

You should regularly update the Linux OS installed on the host virtual machine (VM) running your Service Portal application in order to benefit from the latest fixes and security features. This should be done in a scheduled maintenance window, as it will require shutting down the application while the update takes place.

### *To update the Linux OS*

1. Using an SSH client, establish a connection to the Service Portal using the root username/password.
2. Stop the Service Portal application using the following commands:

```
systemctl stop corero-ssp-backend
systemctl stop corero-ssp-syslog
systemctl stop corero-ssp-services
```

3. (Optional) Take a snapshot of the Service Portal VM using a suitable management utility.
4. Issue the `yum update` command and review the listed updates for suitability.
5. Type "y" and then **Enter** to accept the updates.
6. When all updates are complete, reboot the VM.
7. Restart the Service Portal application using the following commands:

```
systemctl start corero-ssp-backend
systemctl start corero-ssp-syslog
systemctl start corero-ssp-services
```

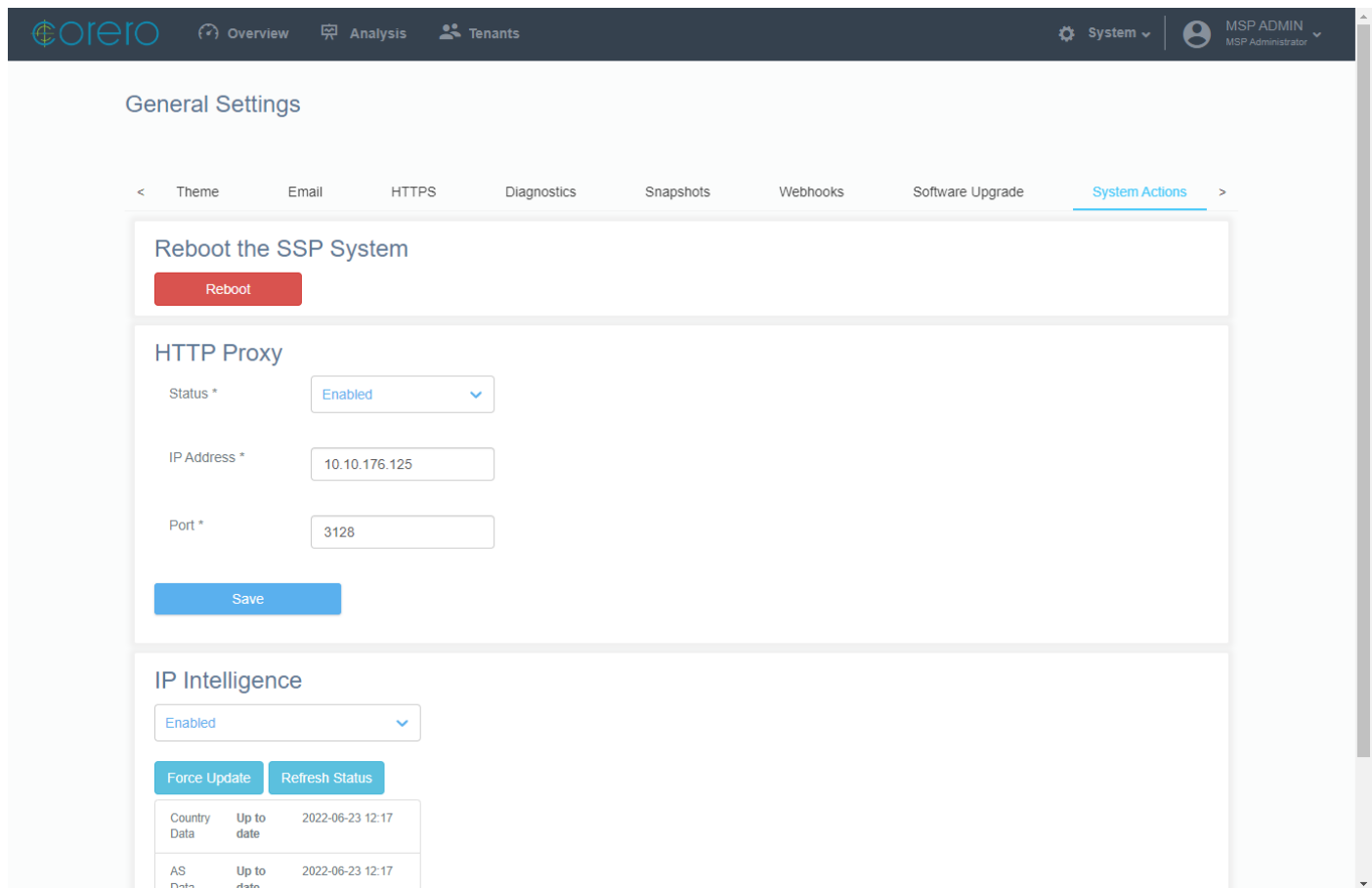
## System Actions

**Note:** Only MSP Administrators can perform system actions.

From this screen you can reboot the Service Portal, manage your connection to the IP Intelligence Smart-Plugin (or service) on the CMS, and manage a HTTP proxy for the Service Portal.

### System Actions screen

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



The screenshot shows the Corero System Actions screen. The top navigation bar includes the Corero logo, Overview, Analysis, Tenants, System (with a dropdown), and MSP ADMIN (MSP Administrator). The main content area is titled "General Settings" and contains a tabbed interface with tabs for Theme, Email, HTTPS, Diagnostics, Snapshots, Webhooks, Software Upgrade, and System Actions (which is currently selected). The System Actions tab contains three sections: "Reboot the SSP System" with a red "Reboot" button; "HTTP Proxy" with fields for Status (set to Enabled), IP Address (10.10.176.125), and Port (3128), and a blue "Save" button; and "IP Intelligence" with a dropdown set to Enabled, buttons for "Force Update" and "Refresh Status", and a table showing data updates.

Country Data	Up to date	2022-06-23 12:17
AS Data	Up to date	2022-06-23 12:17

### Reboot the Service Portal

You can restart the Service Portal application if you encounter any problems.

**Caution:** You will be logged out of the Service Portal.

### *To restart the Service Portal*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **System Actions** tab.
3. Click **Reboot**.
4. Once the Service Portal restarts, you can log back in.

### **Manage IP Intelligence Smart-Plugin status**

The IP Intelligence Smart-Plugin (or service) enables your SmartWall system to associate IP addresses with geographic locations. It is primarily managed in the CMS, but the connection between that Smart-Plugin and the Service Portal requires a periodic sync.

**Note:** You must have the IP Intelligence Smart-Plugin installed on your CMS (or have the equivalent service licensed and enabled in later versions) to access this feature. You must also have DNS configured on the Service Portal VM.

### *To disable the connection to the IP Intelligence Smart-Plugin*

If you do not have the IP Intelligence Smart-Plugin or service enabled, you can disable the sync attempting to pull that information from your SWA.

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **System Actions** tab.
3. In the IP Intelligence area, select **Disabled** from the drop-down.

### *To refresh the status of the IP Intelligence Smart-Plugin or service*

This refreshes the locally stored status.

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **System Actions** tab.
3. In the IP Intelligence area, click **Refresh Status**.
4. Check the status table below to view the new status of the connection.

### *To force an update of the IP Intelligence Smart-Plugin connection*

This pulls an updated status down from the IP Intelligence Smart-Plugin or service.

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **System Actions** tab.
3. In the IP Intelligence area, click **Force Update**.
4. Check the status table below to view the new status of the connection.

## Enable a HTTP Proxy for the Service Portal

If outgoing connections from the Service Portal are routed through an HTTP Proxy then you will need to setup the Service Portal to enable the external connection. This includes the connection used by the IP Intelligence Smart-Plugin or service (if you are using it).

### *To enable a HTTP proxy for the Service Portal*

1. From the main toolbar of the Service Portal, click **System > General Settings**.
2. Open the **System Actions** tab.
3. In the HTTP Proxy area, from the **Status** drop-down, select **Enabled**.
4. Type the **IP Address** of the HTTP Proxy Server.
5. Type the **Port** number for the HTTP Proxy port on your server. The default port is 443.
6. (Optional) Edit the **Connection Timeout** period. The default is 30 seconds.
7. (Optional) Edit the **Read Timeout** period. The default is 30 seconds.
8. Click **Save**.

## Custom Tenant Fields

**Note:** Only MSP Administrators can manage custom tenant fields.

From this screen you can customize the data fields used to store details on the tenants you create in the Service Portal. You can define up to 20 fields, and choose which of these you want to display on the Tenant Status panel when a Tenant is logged in.

Custom fields are created in the form of text-only strings of up to 128 characters, and are applied to all Tenant records on creation. This may result in missing (empty) field values if you already have existing tenants defined. In the case of mandatory fields, any missing values must be entered on the Details tab if you subsequently amend the tenant details using the Tenant Management screen.

Once defined, custom fields will be accessible through the Service Portal interface, REST API and CSV export functions with the following restrictions:

- Custom fields are only accessible (to read or modify) through REST API **v3** calls.
- After upgrading to version 2.1.0, any tenant details which use legacy data fields will be converted to retain the information in an equivalent custom field. The following legacy fields will be converted (if present) to custom fields:
  - `identifier1`
  - `identifier2`
  - `contactName`
  - `contactEmail`

- `contactPhoneNumber`
- `address`

After conversion, REST API v2 calls which attempt to access these fields will work as normal, except for those fields which have not yet been defined (e.g. after a new install) or have subsequently been deleted. Converted fields can be edited (or deleted) like any other custom field after conversion.

- If you wish to [import multiple tenant details](#) using a CSV import, you should ensure that you download and check the structure of the example CSV export, which contains a column header row including any custom fields you have created. Older CSV files which do not follow the currently defined structure will be rejected.









Custom field definition is accessed through the Custom Tenant Fields tab.

### Accessing the Custom Tenant Fields tab

You can navigate to the Schema tab of the General Settings screen by clicking **System > General Settings > Custom Tenant Fields** on the main toolbar.

Custom Tenant Fields

Add Field

Name	Label	Description	Visible to tenants	Mandatory field	Actions
contactName	Contact Name	Contact Name	No	No	 
contactEmail	Contact Email	Contact Email	No	No	 
contactPhoneNumber	Contact Phone Number	Contact Phone Number	No	No	 
address	Address	Address	No	No	 

<

1



>

1 - 4 of 4 results

Show

5

▼

The Custom Tenant Fields list shows all custom fields you have added. You can click **Add Field** to create a new custom field, or click on the  Edit or  Delete icons to amend a field definition or remove it completely.

When adding or amending custom fields, you will be prompted to enter the following information:

**Name** – A required identifier for the custom field, in lowercase with no special characters (other than underscore) or spaces. This name will be used in templates, CSV import/export and REST API calls to identify the field.

**Label** – A required human-readable name which will identify the tenant in the Tenant Management screen and any other part of the Service Portal user interface. The Label is used for display purposes only.

**Description** – An optional description of the purpose of the field, for information only.

**Visible to tenants** – A required field which denotes whether or not the field name and value will be displayed on the Tenant Status panel of the Tenant Overview screen when logged in as a tenant.

**Mandatory field** – A required field which denotes whether or not the field itself is mandatory when creating new tenants, or amending tenant details on the Tenant Management screen.

Click **Save** to complete the process once you have entered the information above.

Once created, a custom field may be amended without changing the data associated with it. However, any REST API calls, report placeholder references or CSV files which access the field may require updating, if, for example, you change the Name identifier.

**Caution:** If you delete a custom field, this will alter the structure used for future CSV import/export operations, and any data associated with the deleted field will be lost. Deleted custom fields will be removed from **all** existing tenants. Deleting a custom field will also invalidate any report templates which refer to it.



## Tenants Overview

A tenant is a customer who has access to the SmartWall Service Portal to view their own traffic data and analyze attacks. They can only view information about the traffic going to the IP addresses you add to their asset list, and manage their own tenant users.

**Note:** The number of tenants you can have depends on your license. The smallest license allows for up to 10 tenants, and the largest allows up to 10,000.

There are two ways to create a tenant. You can [create single tenants](#) directly in the portal, or you can upload a tenant import file to bulk [create multiple tenants](#).

Once you create a new tenant, you need to provide them with at least one Tenant Administrator user account, to enable their portal access. You, other MSP Administrators and MSP Users, or the Tenant Administrator themselves can then create further user accounts for their tenancy (including additional Tenant Administrators). You must also populate their Assigned Asset list with the relevant IP ranges associated with this tenant's Assigned Assets. Once you do this, the portal begins associating traffic with that tenant and populating their charts/tables with information on current and historic attacks against their assets.

You can view all per-tenant information on the Tenant Management screen, by selecting the required tenant from the left-hand side. You can then view a tenant's live attacks and attack history on their dashboard (which is displayed by default). You can also use this view to manage their **Assets** and **Asset Groups**, their **Users**, their **Password** expiry options (if they aren't using the system-wide settings), the **Audit** log for their tenancy, and their service **Details**, by selecting the relevant tab. To find a specific tenant, you can use a combination of the search, sort, and filter options to narrow down the list.

### Tenant traffic and attacks

The SmartWall System forwards the meta data for real-time traffic samples to the Service Portal. On a tenant's **Dashboard**, you can see only the traffic whose destination IP address is on that tenant's [Asset](#) list. The charts and date filters work in exactly the same way as on your [Service Overview screen](#). This is the same information the tenant sees in their Overview screen, when they log into the Service Portal.

## 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). For each tenant, you need to specify which assets in your protected network belong to them.

In the **Assets** tab of the selected tenant panel, you can [add, edit or remove IP addresses which are protected by the service](#). The attack traffic sent against the IP addresses on your tenant's asset list, is the attack traffic which appears on the tenant's dashboard and Attack Analysis charts.

**Note:** An IP address can only be assigned to one tenant. If you try to assign an IP address that has already been assigned to another tenant, you will see an error message and be unable to complete that operation.

There are two ways to assign assets to tenants using the Web UI. Directly in the portal, you can [assign individual assets to a tenant](#) or you can [upload an asset import file](#) to add multiple assets to tenants. An asset you have assigned to a tenant is called an **Assigned Asset** and you can use the Asset View drop-down to view all of a tenant's Assigned Assets.

**Note:** You can give an Assigned Asset a name when you add it, but this is not the same as creating a Named Asset. The Assigned Asset's name is only visible to MSP Administrators and Users, and can be used for purely internal purposes (e.g. a server name or colo).

To enable them track certain IP addresses or ranges, your or your tenants can identify them as **Named Assets**. The name given will appear in charts, alerts, and reports whenever an address in the Named Asset range is attacked. For example, if your tenant has multiple websites, they may want to associate the website names with each IP Address to enable them to quickly spot which website has been attacked. 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.

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

As well as creating Named Assets, you can create asset groups to organize a tenant's assets. Once you create an asset group, you can assign Named Assets to it. For example, your tenant may have a few similar services they want to keep track of together. They 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.

Tenant Administrators are able to create and edit Named Assets from within the range of their Assigned Assets, and they can create and manage their asset groups. However, they are unable to edit the Assigned Assets list.

## Reassigning an Asset

At some point you may find you need to move an Assigned Asset from one tenant to another. You must delete the asset from the first tenant's Assigned Asset list and then create the new asset, with the same IP addresses, in the second tenant's Assigned Asset list. The new tenant will only see attacks against this IP address from the time the new asset is created and won't have any access to the historical attack information associated with the previous tenant. Likewise, the previous tenant will still be able to see their historic attack information for this IP address, but will not have access to any new attack information after the asset was deleted from their list.

## Tenant user roles

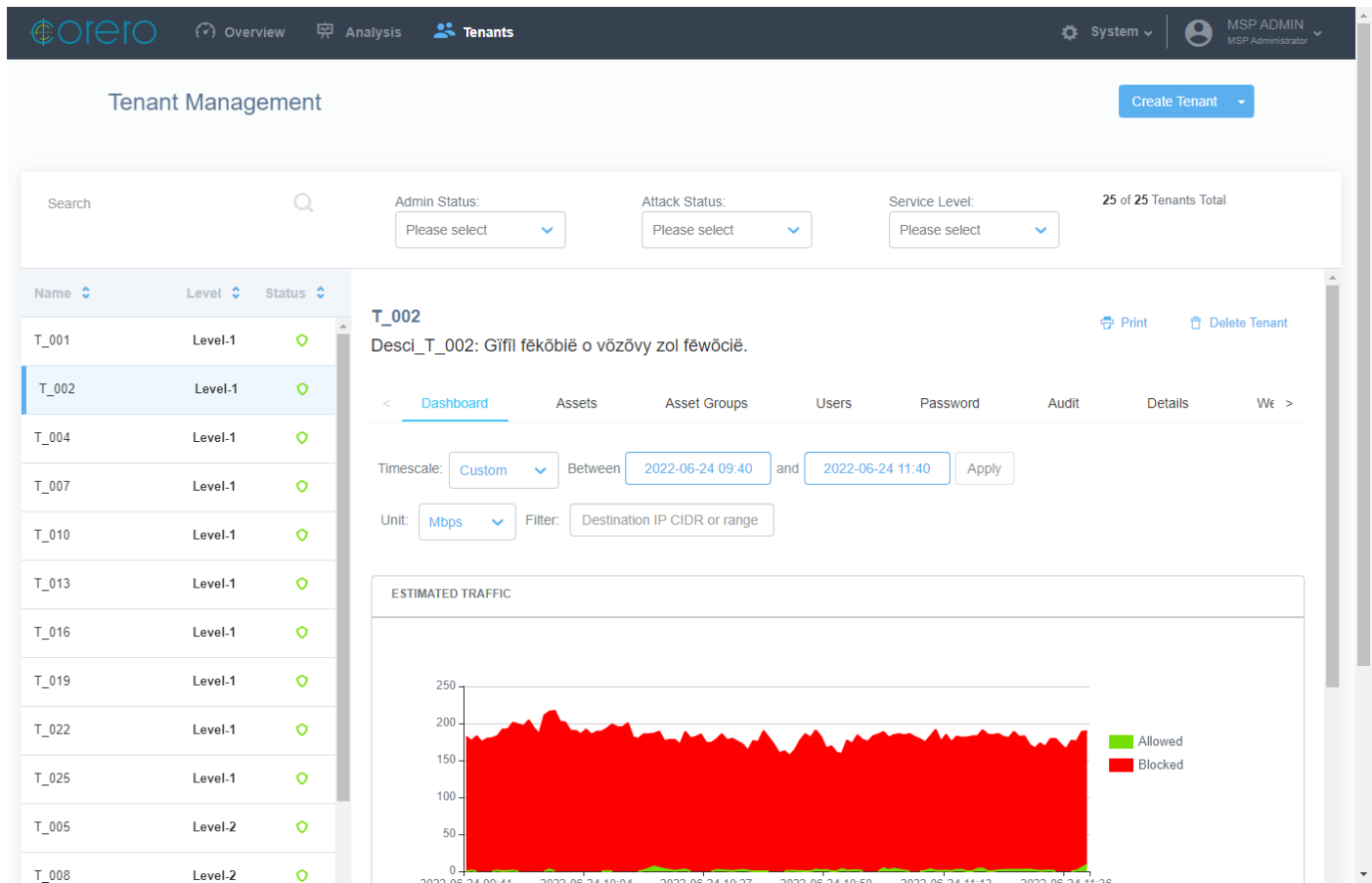
Each tenancy in your Service Portal can have multiple users, each with their own login credentials, with two types of user role available:

- **Tenant Administrator** – Can view traffic data, analyze attacks, manage assets, and manage users.
- **Tenant User** – Can view traffic data, analyze attacks, and manage assets

You can view and [manage the users for a tenancy](#) in the **Users** tab of the selected tenant panel.

## Tenant Management screen

You can navigate to the Tenant Management screen by clicking **Tenants** on the main toolbar.



## Create a tenant

In the top right of this screen you can see the **Create Tenant** button. Click the button to begin creating a new tenant or click the drop-down list next to the button to import multiple tenants or import multiple assets for existing tenants.

## Find a tenant

At the Search bar, type a search term to have the tenants list only display tenants whose information includes that term. You can search all fields using the search bar, including assets. If you need to find which tenant owns a specific IP address, you can type the IP address into the search bar. Or if you need to find which tenant a user belongs to, you can type their name or email address into the search bar.

You can also use the following filters on the tenants list:

- **Admin Status**
  - **Enabled** – The tenant is enabled for DDoS protection
  - **Disabled** – The tenant is not enabled for DDoS protection

- **Attack Status**
  - **Under Attack** – The tenant is currently under attack
  - **Not Under Attack** – The tenant is not currently under attack
- **Service level** – Once you [create Service Levels](#), you can filter the tenants list by selecting only the Service Levels you want to appear

Click the **x** in the filter fields to remove the current filter.

You can use the search bar and filters individually or together, to view specific tenants or a subset of tenants from the full list. As you filter the list, you can see the **Tenants Total** count change (to the right of the filters).

You can sort the tenants list by clicking on the **Name** and **Level** column headers. The carats show whether the list is in ascending or descending order.



### Navigate a tenant's options

Once you select a tenant, you can view their management information in the main part of the screen. You can access the following management tabs:

- **Dashboard** – Much the same as your Service Overview screen but it displays only traffic that is going to the IP addresses on the tenant's asset list. You can filter the information to view specific attacks.
- **Assets** – Contains a list of the assets assigned to this tenant. There are two views available in the **Asset View** drop-down:
  - **Assigned** – All of the IP addresses assigned to this tenant
  - **Named** – The Named Assets created by you or by the Tenant Administrators.
 You can search the list, add new assets, and edit or delete existing assets.
- **Asset Groups** – Enables you to create, edit and delete the asset groups for this tenant.
- **Users** – Contains a list of all the user accounts on this tenancy. You can search the list, add new users, and edit or delete existing ones.
 

You can search the list by first selecting a field to search in using the drop-down, and then typing in a search term. The list is then filtered to only contain users who match the search criteria.
- **Password** – If you don't want this tenant to use the system-wide password expiry settings (**System > Password**), you can override them and set tenant specific settings here. The fields are the same as on the System screen, except you can choose to make them editable by the Tenant Administrators on this tenancy.
- **Audit** – You can view the audit log for this tenancy.
- **Details** – You can view and edit information about the tenant's service and the primary contact.
- **Webhooks** – You can manage your tenant-specific Webhooks. Tenant Administrators can also manage their own Webhooks.

In the top right corner of all of these tabs you have two buttons:

-  **Print** – Enables you to print the information on that tab.
-  **Delete Tenant** – Deletes this tenant. Once you confirm the deletion, you cannot reverse this action.

## Creating a New Tenant

When you create a tenant, you are creating a specific view within the SmartWall Service Portal which displays only the traffic information for a single customer.

Once you create the tenant, you then need to create a Tenant Administrator account and add a list of their Assigned Assets. They can then log in, view their traffic data, analyze attacks and manage their tenant users.

**Note:** If you need to [create multiple tenants](#) quickly, you can import their details in a text file rather than using the Create Tenant options.

### Prerequisites

Before creating your first tenant, make sure that you have:

- [Configured your service policy](#)
- [Added a logo to the Service Portal](#)

### To create a new tenant

1. From the main toolbar of the Service Portal, click **Tenants**.
2. Click **Create Tenant**.
3. Enter the following information:
  - **Tenant Name** – The name of the new tenant
  - **Tenant Description** – Write a short description of the tenant that will appear below the Tenant Name when you view their details and on the tenant's Service Overview screen. This must be at least 6 characters long.
  - **Service Level** – Once you have set up your [service policy](#), use the drop-down to select the level this tenant has subscribed to.
  - **Country** – (Optional) Type which country the primary contact is based in.
  - **Status** – By default, this is set to **Enabled**. If you want to create a tenant now and then enable them in the future, you can select **Disabled**.
4. Click **Save**.

**Note:** Any custom tenant fields you have defined in the [Custom Tenant Fields tab](#) will also be presented for data entry on this screen.

### Next Steps

Once you have created the tenancy, you must [create a Tenant Administrator](#) with log in credentials. You can then pass the account details on to your customer so they can begin to manage their own tenancy. You now need to [set up the tenants Assigned Assets](#) so they can see their traffic.

## Importing Multiple Tenants

If you have a list of tenants you need to create at the same time, you can import a text file containing each tenant's details. The Service Portal then creates a tenancy for each tenant on that list.

### To import multiple Tenants

1. From the main toolbar of the Service Portal, click **Tenants**.
2. Click the drop-down arrow next to Create Tenant.
3. Click **Import Tenants**.
4. Click **Download**. The example import file is downloaded through your browser.
5. Open the example file (tenants.csv) using a plain text editor (Notepad, Emacs, etc).
6. Update the example content with your Tenant information, and then save the file.

**Note:** The file must be saved as a .csv file, and it must be 3MB or less.

7. Return to the Service Portal. If you had to close your session, first click **Tenants > Create Tenant** drop-down to return to the Import screen.
8. Chose whether you want to **Overwrite existing Tenants** with the imported content:
  - Select the check box to merge the imported assets with the existing Tenant List and, for any imported tenants which match an existing tenant, overwrite with the imported version.
  - Or leave the box unchecked to merge the imported tenants with the existing tenant list and highlight any merge conflicts without overwriting the existing tenants.
9. Click **Import Tenants**.
10. Locate and select your updated `tenants.csv` file, and then click **Open**.
11. You can now see your new tenants in the Tenant List.

**Note:** If there was a problem with any of a tenant's information (e.g. missing double quote, unexpected text value etc), none of the tenants will be imported. Instead, you will see a red error message indicating the row number and some error details.

### Editing a Tenant import file

When you're importing tenants into the Service Portal, you can modify the example tenant import file to import your tenant's details. To do this successfully the file must adhere to the following standards:

**Caution:** You must only edit import files in a plain text editor (Notepad, Emacs, etc) or Excel. Do not edit in Word; this can corrupt the information. For example, the straight quotes (") in the template may be converted to curly quotes (”), this would corrupt the information and stop the assets being imported.



- The file can contain up to 1000 rows. If you have more than 1000 tenants to add, you must use multiple import files.
- When you edit the example tenant import file, you must not delete the header row. Use the header row labels as a guide to entering subsequent data rows as follows:
  - **name** – The name of a tenant (as you want it to appear in the tenant's Service Portal interface).
  - **description** – A description of the tenant (as you want it to appear in the the Tenant's Service Portal interface).
  - **servicePolicy** – The policy level you want to assign to this tenant.
  - **status** – Set to **ENABLED** to enable your tenant on creation, or set to **DISABLED** to create an inactive tenant (you may choose to enable the tenant at a later date).
  - **country** – The country your tenant resides in.
- Enter any further custom fields you previously created on the [Custom Tenant Fields tab](#), following the header names which appear in the generated example.
- If a field contains a comma (,) or new line character, the field must be surrounded by double quotes (")
- If a field contains double quotes ("), the double quote must be escaped with another double quote, and then the field must be surrounded by double quotes. For example, to add `hello "world"` to the field, you would need to write `"hello ""world"""`.
- Fields must be separated by a comma (,).

## Next steps

You need to [assign assets](#) to your new tenants. You can use the [import assets](#) feature to bulk assign assets to multiple tenants.

## Managing a Tenant's Users

A tenancy can have multiple user accounts who can access their SmartWall Service Portal area. When you first create a new tenant, you must create at least one Tenant Administrator so your customer can log in to their tenancy.

You can use the **Search** field to filter the user list to only show results which contain the search term.

**Note:** Tenant Administrators can also manage users from within their tenancy.

### To add a new user

1. From the main toolbar of the Service Portal, click **Tenants**.
2. From the tenant list, select the tenant you want to edit.
3. In the selected tenant panel, click the **Users** tab.
4. Click **Create User**.
5. 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.
  - **SSO Only** - Select this option to restrict the user to using [Single Sign-On](#) for authentication.
  - **Phone** – 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 receiving emails about specific alerts or reports.
6. Click **Save**.
7. Provide the new Tenant Administrator with their log in details.

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

## Managing a Tenant's Assets

**Note:** Tenant Administrators are also able to manage Named Assets and Asset Groups. However, they are unable to edit the Assigned Asset list.

For the SmartWall Service Portal to know which traffic relates to a specific tenant, it requires a list of IP addresses, referred to as assets, that are associated with that tenant.

**Note:** IPv6 addresses should be formatted in lower case, and use compressed notation. For example, the address `2001:db8:0:0:1:0:0:1` would be written in compressed notation as `2001:db8::1:0:0:1`

You can view all assigned assets or just the named assets, by selecting from the **Asset View** drop-down. You can also use the **Search** field to filter the asset list to only show results which contain the search term.

**Tip:** You can use the Search field to look for a single IP Address within an asset's address range to view that asset.

### To add a new Assigned Asset

**Note:** If you need to [create multiple assets](#) quickly (for multiple tenants), you can import their details in a text file rather than using the **Create Tenant** drop-down.



1. From the main toolbar of the Service Portal, click **Tenants** .
2. From the tenant list, select the tenant you want to edit.
3. In the selected tenant panel, click the **Assets** tab.
4. From the Asset View drop-down, select **Assigned**.
5. Click **Add Asset**.
6. Type in the **IP Address** (single address/range/subnet) you want to associate with this tenant.
7. (Optional) Provide an **Name** to identify this asset. This name is only visible to other MSP Administrators and MSP Users. It does not make this a Named Asset.
8. Click **Save**.

**Note:** You can edit  or delete  assets from the Asset table.

### To add a new Named Asset

1. From the main toolbar of the Service Portal, click **Tenants** .
2. From the tenant list, select the tenant you want to edit.
3. In the selected tenant panel, click the **Assets** tab.
4. From the Asset View drop-down, select **Named**.
5. Click **Add Asset**.


6. Type in the **IP Address** (single address/range/subnet) you want to identify as a Named Asset.
7. Type a **Name** to identify this asset.
8. (Optional) Select an Asset **Group** the new Named Asset will belong to.
9. Click **Save**.

**Note:** You can edit  or delete  Named Assets from the Named Asset table. Deleting a Named Asset does not affect any of the Assigned Assets for this tenant.

### To create an asset group

You can't add an asset to a group, unless the tenant has existing asset groups.

1. From the main toolbar of the Service Portal, click **Tenants**.
2. From the tenant list, select the tenant you want to edit.
3. In the selected tenant panel, click the **Asset Groups** tab.
4. Click **Create Asset Group**.
5. Type a **Name** for this new group.
6. Click **Save**.

**Tip:** You can use the edit () and delete () buttons to manage asset groups.

## Importing Multiple Assets

Once you create a tenant, you need to assign assets to them before they can begin seeing traffic. If you have multiple new tenants, that you need to assign assets to, you can save time by importing a list of those assets rather than assigning each one using the Web UI. You can use this feature to create Assigned Assets and/or Named Assets.

### Prerequisites

You must [create the tenants](#) you want to assign assets to. (You can [import tenants](#) in a similar way to bulk create multiple new tenants)

### To import multiple assets

1. From the main toolbar of the Service Portal, click **Tenants**.
2. Click the drop-down arrow next to Create Tenant.
3. Click **Import Assets**.
4. Click **Download**. The example import file is downloaded through your browser.
5. Open the example file (assets.csv) using a plain text editor (Notepad, Emacs, etc).
6. Replace the example content and save the file.

**Note:** The file must be saved as a .csv file, and it must be 3MB or less.

7. Return to the Service Portal. If you had to close your previous session, then from the drop-down arrow next to **Create Tenant**, click **Import Assets**.
8. In the Import dialog, chose whether you want to **Create Asset Groups if they do not exist**. This creates a new asset group for any Asset Group names in the import file which don't match an existing Asset Group name.
9. Chose whether you want to **Overwrite existing Assets** with the imported content:
  - Select the check box to merge the imported assets with the existing asset list and, for any imported assets which match an existing asset, overwrite with the imported version.
  - Or leave the box unchecked to merge the imported assets with the existing asset list and highlight any merge conflicts without overwriting the existing assets.
10. Click **Import Assets**.
11. Locate and select your updated assets.csv file then click **Open**.
12. Now, when you open a tenant's asset list, you should see the new assets.

**Note:** If there was a problem with any of the asset information (e.g. missing double quote, unexpected text value etc), you will see a red error message and none of the assets will be imported.

## Editing an asset import file

When you're importing asset information into the Service Portal, you can modify the example asset import file to import your existing tenant's names and asset IP addresses. To do this successfully the file must adhere to the following standards:

**Caution:** You must only edit import files in a plain text editor (Notepad, Emacs, etc) or Excel. Do not edit in Word; this can corrupt the information. For example, the straight quotes (") in the template may be converted to curly quotes (”), this would corrupt the information and stop the assets being imported.

- The file can contain up to 1000 rows. If you have more than 1000 assets to add, you must use multiple import files.
- In each row, you need a tenant name (as it appears in the service portal) and the IP address of the asset you want to assign. In the first row of the example import file you can see the following field to help you craft your own list:
  - **"TenantName1"** – Replace the text with the name of a tenant (as it appears in the service portal)
  - **ASSIGNED** or **NAMED** – Choose the correct asset type: ASSIGNED for creating Assigned Assets, and NAMED to create Named Assets within an Assigned Asset range.
  - **"assetname"** or **named asset**– (Optional) Replace the text with the name you want to give this asset
  - **asset group** – **Only allowed for NAMED assets** (Optional) Replace the text with the name of the existing asset group you want this asset to be associated with
  - **127.2.1.1** – Replace the example IP address/range/subnet with the asset you want to assign to that tenant

**Note:** IPv6 addresses should be formatted in lower case, and use compressed notation. For example, the address `2001:db8:0:0:1:0:0:1` would be written in compressed notation as `2001:db8::1:0:0:1`

- Each row can only contain one asset. An asset can be a single IP address, range or subset.
- You can't assign an IP address to more than one tenant.
- If a field contains a comma (,) or a new line character, the field must be surrounded by double quotes (").
- If a field contains double quotes ("), the double quote must be escaped with another double quote, and then the field must be surrounded by double quotes. For example, to add `hello "world"` to the field, you would need to write `"hello ""world"""`.
- Fields must be separated by a comma (,). If you chose not to include the **assetname** and **asset group** fields, you must still include the field separating commas for those fields (see second row of the import assets template).

## Viewing Tenant Attacks

A tenant's dashboard is very similar to the Service Overview screen, except that it only shows attack information for the selected tenant. This is also what the tenant sees, when they log into the SmartWall Service Portal.

### Prerequisites

Before you can view a tenant's traffic data, they must have at least one asset in their [Assigned Asset list](#).

### To view a tenant's dashboard


1. From the main toolbar of the Service Portal, click **Tenants**.
2. From the tenant list, select the tenant you want to edit.
3. In the selected tenant panel, if it's not already displaying, click the **Dashboard** tab.
4. Use the date filters to select the time period you want to view:
  - **Timescale** – Use the drop-down to select a preset time scale:
    - **Last Hour** – (Default) 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 charts and table below then show only data from that time period.
5. (Optional) Use the Destination IP CIDR or range **Filter** to show only the specified DIP, CIDR, or range on the charts.

6. View traffic for that time period in the following charts:

- **INBOUND TRAFFIC** – Displays the inbound traffic (in megabits per second) for this tenant during the selected time period.

The green area on the chart denotes allowed traffic from the SmartWall Threat Defense System (SmartWall TDS) 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 out to cover the whole chart to once again view the entire selected time period.

- **TOP ATTACKED IP ADDRESSES** – Displays the IP addresses (associated with this tenant) that received the most attacks during the selected time period. The exact number of attacks is displayed at the end of each bar.
- **ATTACKS** – Displays every attack on this tenant during the selected time period. In the top right corner you can see the total number of attacks 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 Group** – If the asset is part of a group, this is displayed here. Otherwise this field is blank.
  - **Asset Name** – If the attacked IP address is part of a Named Asset, the name is displayed here. Otherwise this field is blank.
  - **IP Address** – The IP address which is the target of the attack
  - **Attack Status** – An attack can be **Ongoing** or **Completed**
  - **Start Time** – The time that the attack traffic was first detected by the SmartWall TDS
  - **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 by the SmartWall TDS.
  - **Peak (Mbps)** – For an ongoing attack, this field shows the highest rate of attack traffic (in megabits per second) detected so far during the attack. For a completed attack it shows the highest rate of attack traffic detected during the whole attack.
  - **Attack Volume** – The volume of traffic sent over the duration of this attack.

## Viewing Tenant Audit Log

In the tenant area, you can view an audit log to see a list of every user action performed on a specific tenancy.

### To view a tenant's Audit Log

1. From the main toolbar of the Service Portal, click **Tenants**.
2. From the tenant list, select the tenant you want to view.



3. In the selected tenant panel, click the **Audit Log** tab.

4. Use any of the filters to refine the actions displayed:

- 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)
  - **MSP Roles** – Show or hide all actions performed by MSP Administrators and MSP Users
  - **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.

### To export a tenant's 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.

1. From the main toolbar of the Service Portal, click **Tenants**.
2. From the tenant list, select the tenant you want to view.
3. In the selected tenant panel, click the **Audit Log** tab.
4. Apply any filters you require to the Audit Log.
5. Click **Export**.
6. A .csv file of the filtered Audit Log will now download in your browser

## Managing Tenant-specific Notifications

**Note:** This feature is only available to MSP Admin and Tenant Admin users when enabled by an MSP Admin on the **System > Policy and Reporting > Policy** tab.

Tenants can manage their own alert notifications (email and Webhook) in their System menus. However, you can also help to manage the notifications for specific tenants.

**Note:** Tenant-specific notifications will only send alerts about that Tenant's traffic.

To access the currently configured notifications for a Tenant, follow these steps:

1. From the main toolbar of the Service Portal, click **Tenants**.
2. From the tenant list, select the tenant you wish to amend or view.
3. In the selected tenant panel, click the **Notifications** tab.

You can now amend, delete or create notifications as described in [Notification Settings](#). Any changes you make to the notification configuration will only affect the selected tenant.

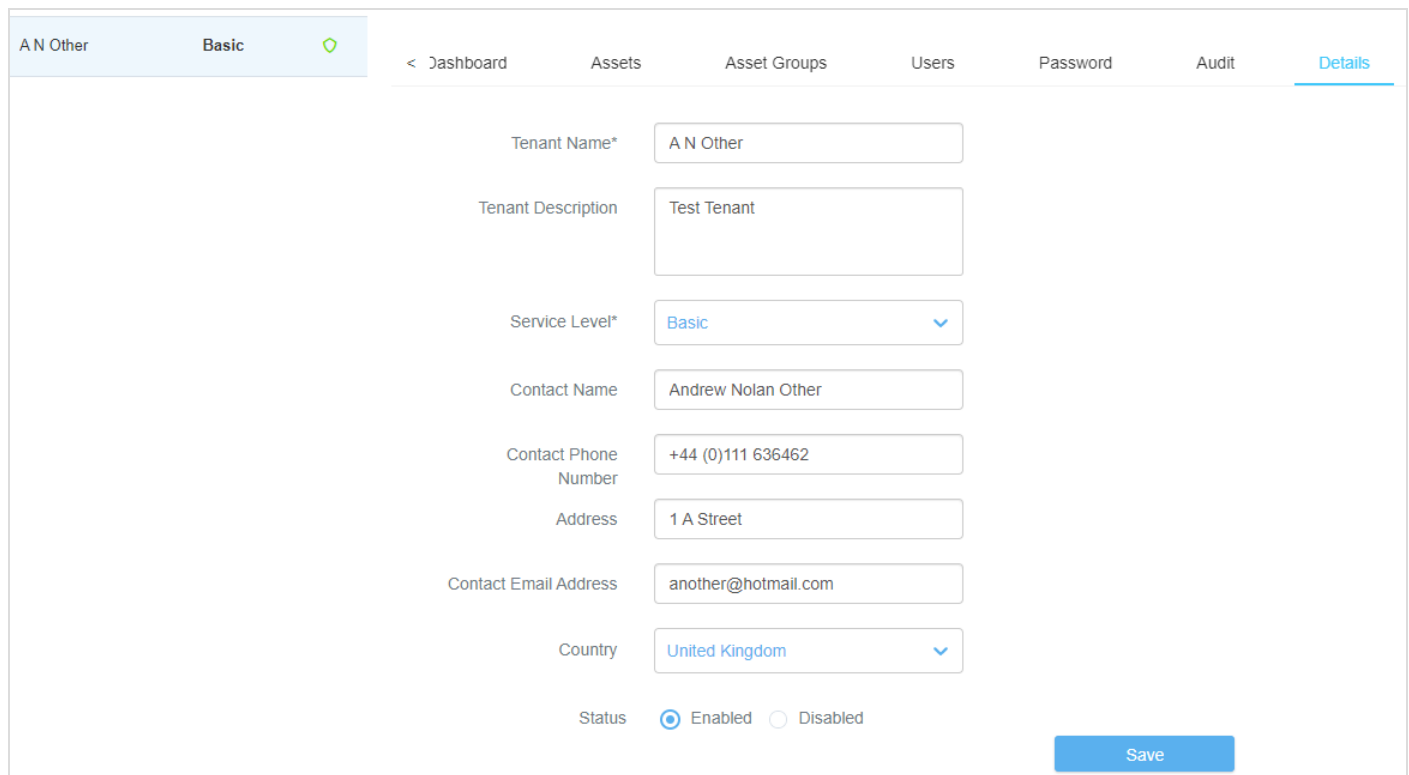
## Changing Tenant Details

You can change the details associated with an existing tenant on the Details tab of the [Tenant Management](#) screen.

### Accessing the Details tab

You can navigate to the Details tab of the General Settings screen by clicking **Tenants** on the main toolbar, selecting the tenant you wish to amend from the list of displayed tenants in the left-hand column, and then click **Details**.

You will see the currently selected tenant's details appear. From this screen you can change any of the details associated with the selected tenant, and then click **Save**.



The screenshot shows the 'Details' tab for a tenant named 'A N Other'. The interface includes a top navigation bar with tabs: 'A N Other', 'Basic', and a green shield icon. Below this is a secondary navigation bar with links: '< Dashboard', 'Assets', 'Asset Groups', 'Users', 'Password', 'Audit', and 'Details' (which is highlighted). The main content area contains the following fields:

- Tenant Name\***: Text input field containing 'A N Other'.
- Tenant Description**: Text input field containing 'Test Tenant'.
- Service Level\***: Dropdown menu with 'Basic' selected.
- Contact Name**: Text input field containing 'Andrew Nolan Other'.
- Contact Phone Number**: Text input field containing '+44 (0)111 636462'.
- Address**: Text input field containing '1 A Street'.
- Contact Email Address**: Text input field containing 'another@hotmail.com'.
- Country**: Dropdown menu with 'United Kingdom' selected.
- Status**: Radio buttons for 'Enabled' (selected) and 'Disabled'.

A blue 'Save' button is located at the bottom right of the form.

When you are changing the details for a tenant, you should note the following points:


- Changes made to the **Tenant Name** and **Tenant Description** fields will appear on the [Tenant Management](#) and [Service Overview](#) screens, and any exported CSV files or reports which contain tenant-specific information.
- Any [custom tenant fields](#) you have defined will appear on this tab.

- Mandatory fields (marked with an asterisk) - including required custom fields - which are currently blank must have a value entered before you can save any changes.
- Changing the **Service Level** will affect the type of service the tenant receives according to the service policy you have set (see [Policy and Reporting](#)).
- Changing the **Status** of a tenant will immediately enable (or disable) their access to the Service Portal and should be used with care. When disabled, neither the Tenant Administrator or any defined users will have access, although you will still be able to view the tenant details and re-enable the tenant if required at a later date.

## Deleting a Tenant

You can chose to delete a tenant, perhaps once they no longer have Assigned Assets in your network.

### To delete an existing tenant

1. From the main toolbar of the Service Portal, click **Tenants**.
2. From the tenant list, select the tenant you want to delete.
3. In the top right corner of the selected tenant panel, click  **Delete Tenant**.
4. Click **OK**.

## Service Overview and Attack Analysis

You can use the Service Overview and Attack Analysis screens of the SmartWall Service Portal to analyze DDoS attacks against your network.

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

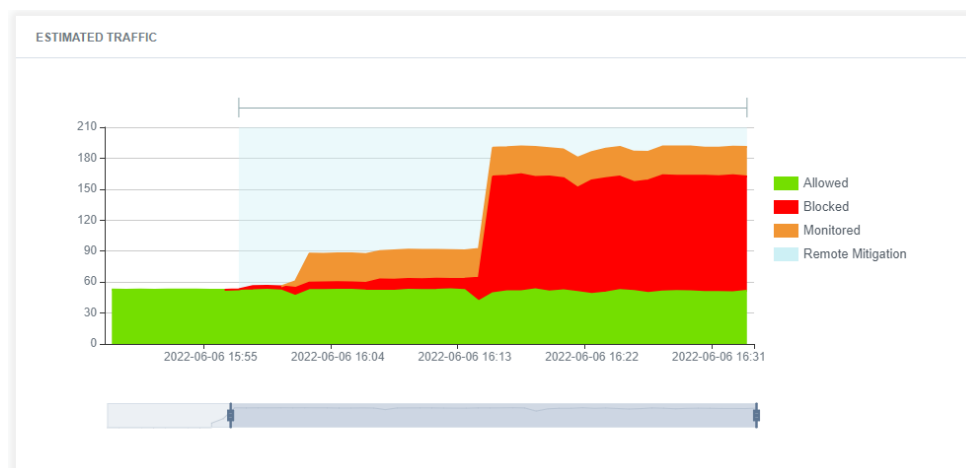
The Attack Analysis screen enables you to search more specifically for attacks, and filter those results by date range. For example, if you were looking for an attack that happened yesterday to an asset called Server1, you could select **Asset Name** from the drop-down list and then type "Server1" into 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 tenant. 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.

### Traffic charts

On the Service Overview and Attack Analysis screens, you can see charts displaying your estimated traffic rate.



The total estimated traffic rate is shown by the height of the graph in either Megabits Per Second (**Mbps**) or Packets Per Second (**PPS**) depending on the **Units** filter you have selected for this screen. Within that total rate, it is broken down by how the traffic has been handled:

- **Green** – Non-attack traffic which has been **allowed** to continue to your tenant's protected assets.
- **Red** – Potential attack traffic which has been **blocked** from reaching your tenant's protected assets.
- **Orange** – Potential attack traffic which has not been blocked. This traffic is being **monitored** but is still allowed to continue to your tenant's protected assets.
- **Blue** – Only available when connected to a SmartWall TDD system. The traffic has been **redirected** by a mitigation configured on the router.

If you have **Remote Mitigation** display enabled, you may see some time periods shaded **light blue**. This indicates that an upstream Remote Mitigation may be affecting your traffic during this time period. You can [choose what display name is shown for different types of Remote Mitigations](#). You can also [choose which types of Remote Mitigations are shown to Tenants](#) and which are only shown to your MSP Admins/Users.

If you are using SmartWall TDD, you may also see some time periods with **grey crosshatching**. This indicated that some traffic data is **Not Available** during this time period.

### Traffic considerations for Service Portals connected to a SmartWall TDD system

The SmartWall systems handle traffic by applying Rule Actions. The SmartWall TDS system has three possible Rule Actions: **Block**, **Detect**, or **Disabled**. In the Service Portal you can see all traffic affected by a Block Rule Action as the red blocked traffic in traffic charts. The traffic affected by Detect or Disabled is allowed to pass to the protected network and appears as green on the Service Portal traffic charts.

The SmartWall TDD system also uses these Rule Actions, and also provides additional Rule Actions specific to mitigating traffic using edge routers: **Redirect**, **Policer**, and **Ignore**. Traffic affected by the Ignore Rule Action are allowed - these appear as green on the Service Portal traffic charts, while traffic affected by the Redirect action are shown with a blue trace. The Policer Rule Action is more flexible and can be used to block or allow traffic. Traffic blocked by a Policer Rule Action will appear as red (blocked), while allowed traffic will appear as orange (monitored).

Rule Action	SmartWall TDS	SmartWall TDD
<b>Block</b>	Blocked (attack records)	Blocked (attack records)
<b>Detect</b>	Allowed (no attack records)	Monitored (no attack records)
<b>Disabled</b>	Allowed (no attack records)	Allowed (no attack records)
<b>Redirect</b>	n/a	Redirected (attack records)
<b>Policer</b>	n/a	If the Policer has allowed traffic, this is shown as Monitored. If the Policer has blocked the traffic, this is shown as Blocked (attack records).

Rule Action	SmartWall TDS	SmartWall TDD
Ignore	n/a	Allowed (no attack records)

### Differences between the Service Portal and SmartWall TDD attack charts

Traffic charts showing blocked and allowed traffic are used in the Service Portal and in the SmartWall TDD SWA application. The charts will appear similar but, as they have different purposes, may display with some differences. The SWA application is used to identify and handle the different attacks, therefore it shows each attack vector as a separate attack. As the Service Portal provides per-tenant traffic analysis, it groups attacks by Destination IP address. Due to this difference, there may appear to be more attacks showing in the SWA application than in the Service Portal for the same time period.

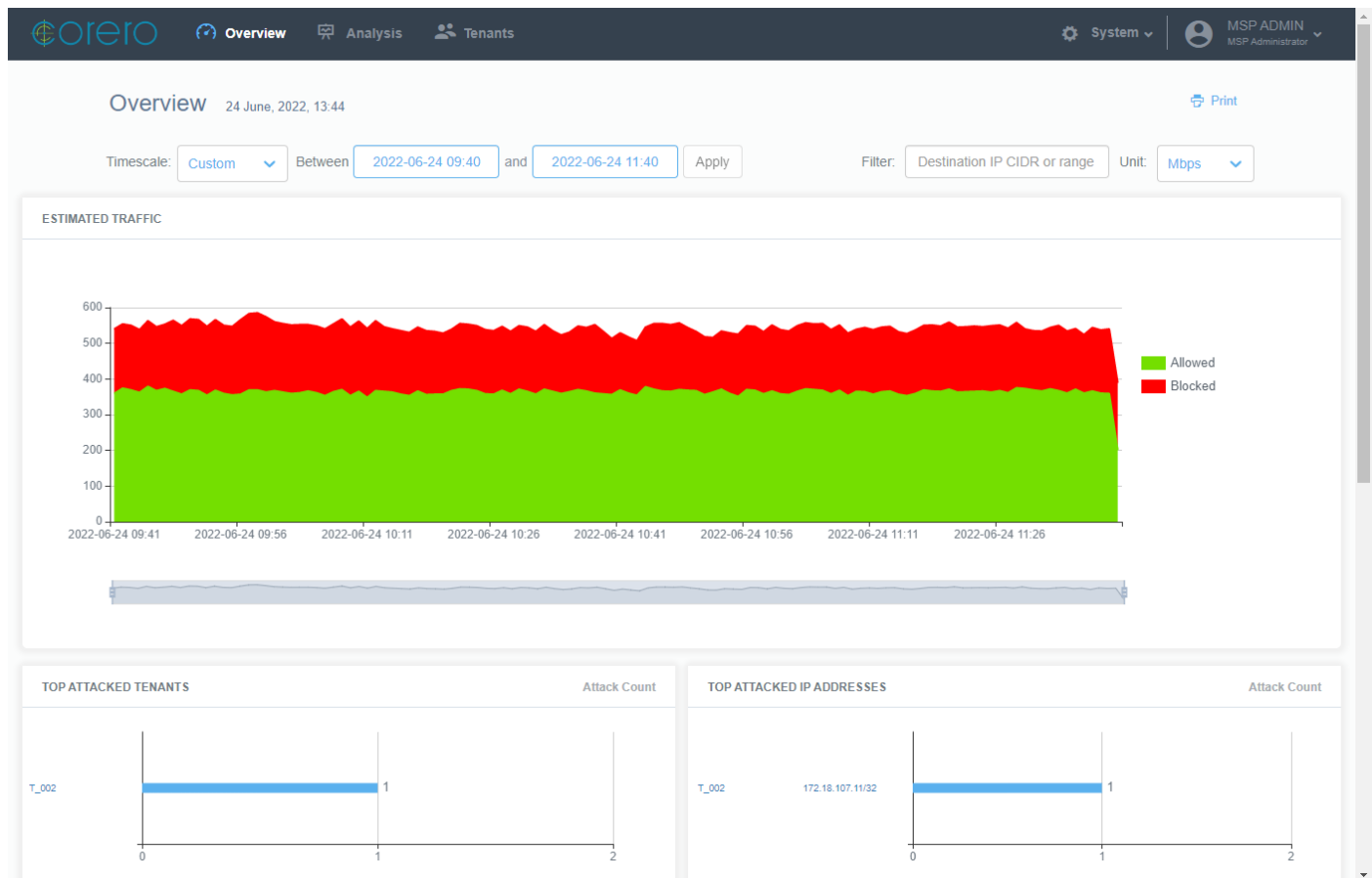
Additionally, charts in the Service Portal and charts in the SWA application independently calculate attack timeout. This can lead to some minor differences in attack duration when comparing the two.

### 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.



## 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 **Unit** filter enables you to display traffic rates in Megabits Per Second (**Mbps**) or Packets Per Second (**PPS**).

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



If you have Remote Mitigation display enabled, you will also have a **Remote Mitigation** filter. You can use this to view **ALL**, **NONE**, or specific Remote Mitigations.


## Charts and tables

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

- **ESTIMATED TRAFFIC** chart – Displays the estimated allowed inbound traffic and estimated blocked traffic for your protected network, over the selected time period.  
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 the keys (**Allowed**, **Blocked**, **Monitored**, **Remote Mitigation**) to the 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 TENANTS** chart – Displays the 5 tenants that received the most attacks during the selected time period. The exact number of attacks is displayed at the end of each bar.
- **TOP ATTACKED IP ADDRESSES** chart – Displays the 5 IP addresses (prefixed by the associated tenant name) 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 network 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.

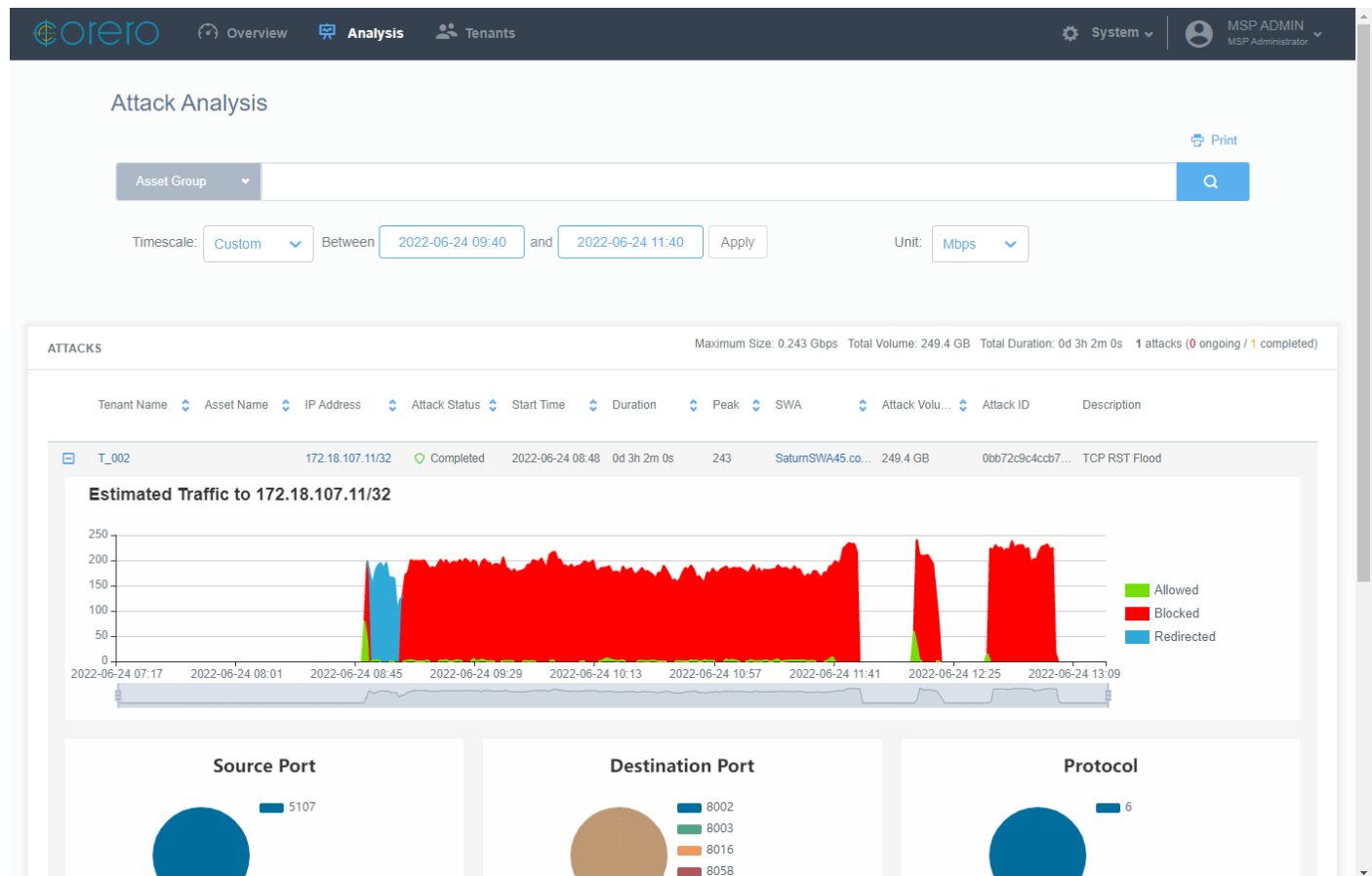
The Attacks table displays the following information for each attack:

- **Tenant Name** – The name of the tenant organization associated with the IP address that is the target of the attack. Click to view all attacks against this tenant. If the customer name is "Default", the attack was against an IP address in your network which is not assigned to any tenants.
  - **Asset Name** – If the IP address is part of a named asset (in the tenant's asset list) this is displayed here. Otherwise, this field is blank.
  - **IP Address** – The IP address or CIDR 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 by the SmartWall TDS
  - **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 by the SmartWall TDS.
  - **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).
  - **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.
- **REMOTE MITIGATIONS** – If you have Remote Mitigation display enabled, you can see a list of the Remote Mitigations affecting your traffic. The table displays the following information for each Remote Mitigation:
    - **Tenant Name** – The name of the tenant organization associated with the IP address that is the target of the Remote Mitigation.
    - **Asset Name** – The name of the asset being affected by this Remote Mitigation.
    - **Asset IP** – The specific IP addresses within that Asset, which are affected by this Remote Mitigation.
    - **Destination** – The destination address/subnet targeted by the Remote Mitigation.
    - **Status** – The current status: **Ongoing** or **Completed**
    - **Mitigation Start Time** – The time and date this Remote Mitigation began.
    - **Mitigation End Time** – If it is completed, this shows the time and date when the Remote Mitigation ended. If this is an ongoing mitigation, it will show **N/A**.
    - **ID** – The unique ID associated with this Remote Mitigation.
    - **Remote Mitigation** – The name of the Remote Mitigation.

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.



## Filters

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:

- **Tenant Name** – The Attacks table only shows results that include the search term in the Tenant Organization field.
- **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.
- **SWA** – If you have more than one SmartWall SecureWatch Analytics (SWA) application connected to the Service Portal, you can filter the Attacks table to show only the attacks originating from a SWA whose name matches the search term you enter.

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.


The **Unit** filter enables you to display traffic rates in Megabits Per Second (**Mbps**) or Packets Per Second (**PPS**).

## Charts and tables

The Attacks table displays every attack that matches the search term and which occurred during the selected time period. In the top right corner you can see the total number of attacks broken down into ongoing and completed. You can re-order the table using the column headers and refresh the table to get the latest information using the refresh icon next to the table title.

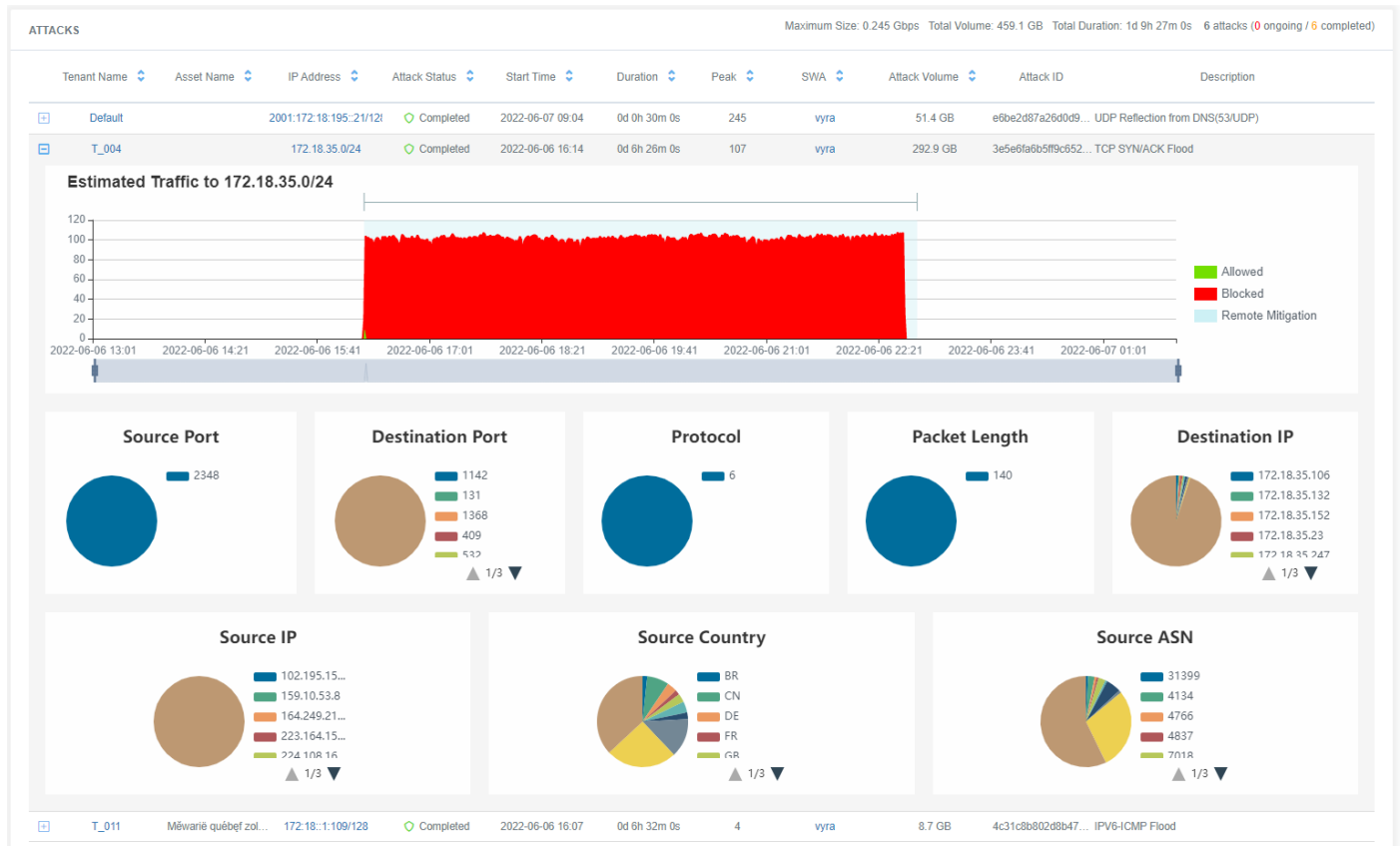
At the top of the Attacks table, you can view a summary of the current table content. This shows the **Maximum Size** of attacks, **Total Volume** of all attacks, **Total Duration** of the attack period shown in the table, and the number of **attacks** listed broken down into **ongoing** and **completed**.

The Attacks table displays the following information for each attack:


-  – Click the expand icon to view an Inbound Traffic chart for the period of the selected attack.
- **Tenant Name** – The name of the tenant organization associated with the IP address that is the target of the attack. Click to open the Tenant Management screen at that customer's dashboard.
- **Asset Name** – If the IP address is part of a named asset (in the tenant's asset list) this is displayed here. Otherwise this field is blank.
- **IP Address** – The IP address or CIDR which is the target of the attack. Click to open the Tenant Management screen at that customer's asset list.
- **Attack Status** – An attack can be **Ongoing** or **Completed**
- **Start Time** – The time that the attack traffic was first detected by the SmartWall TDS
- **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 by the SmartWall TDS.
- **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).
- **SWA** – The name of the SmartWall SecureWatch Analytics (SWA) application where the attack data originated. If you only have one SWA connected to the Service Portal, this column will always show "default" as the SWA name.
- **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**.
- **Attack ID** – A unique ID which identifies this attack. You can use this when discussing a specific attack with the tenant. You can also search for an attack ID in SmartWall SecureWatch Analytics.

- **Description** – A summary of the attack characteristics. If the description is truncated, hover over it to see the full text.

The expanded attack information for a single attack contains the following charts:



- **Estimated Traffic** – It works in the same way as the [Estimated Traffic chart](#) on the Service Overview screen. A focused time line for the attack is shown. The time line has 50% of the total attack time either side of the attack to show it in context.
- **Source Port** – Displays the estimated top source ports seen in this attack.
- **Destination Port** – Displays the estimated top destination ports seen in this attack.
- **Protocol** – Displays the estimated top protocols seen in this attack.
- **Packet Length** – Displays the estimated top packet lengths seen in this attack.
- **Destination IP** – Displays the estimated top destination IP addresses seen in this attack.
- **Source IP** – Displays the estimated top source IP addresses seen in this attack.
- **Source Country** – (Only available with IP Intelligence enabled in the CMS) Displays the estimated top source countries seen in this attack.
- **Source ASN** – (Only available with IP Intelligence enabled in the CMS) Displays the estimated top source ASNs seen in this attack.

**Tip:** You can click  [Print](#) in the top right to print the selected view or save it in PDF format.

## Common Analysis Tasks

On the Service Overview and Attack Analysis screens of the SmartWall 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 in your network

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 tenants who experience the most attacks today

1. From the main toolbar of the Service Portal, click **Overview**.
2. From the **Timescale** drop-down select **24 Hours**.
3. Look at the **TOP ATTACKED TENANTS** chart. Here you can see a visualization of the top 5 most attacked tenants in your network. You can see the exact number of attacks each experienced at the end of the blue bar.

### 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 tenant

On the Service **Overview** screen, if you can see the tenant's name in the **ATTACK** table, you can click it to view a list of all the attacks made against this tenant. Otherwise:

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

1. From the main toolbar of the Service Portal, click **Analysis**.
2. From the Search drop-down, select **Tenant Name**.
3. In the search bar, type the name of the tenant 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 Tenant 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 your require then click Print again.
7. You will print a report listing all the attacks directed at that IP address over the last week.

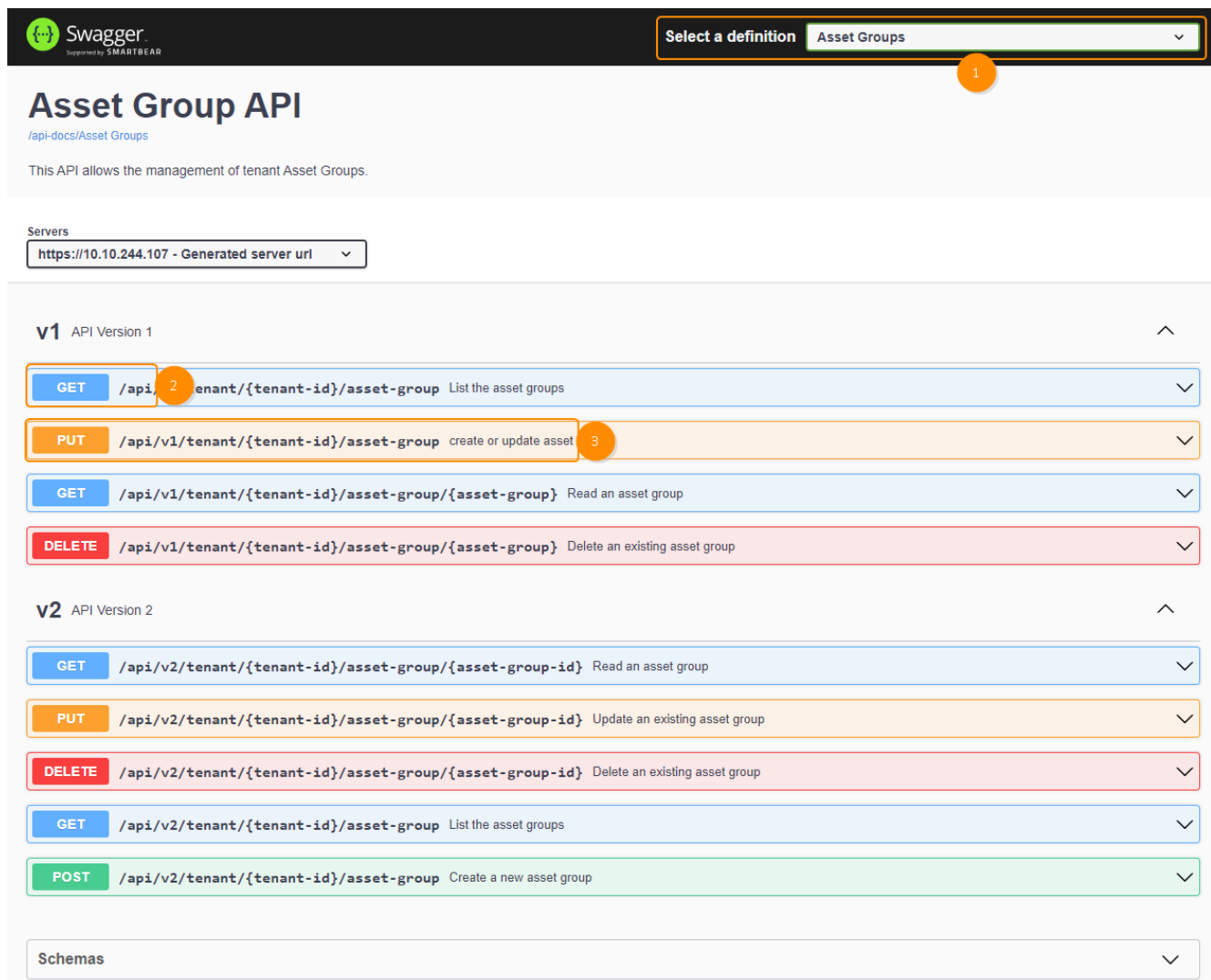
## Service Portal REST API Overview

The documentation for the REST API is accessed in your browser using the Swagger web interface. You can test individual REST commands through the Swagger interface.

### Accessing the REST API documentation

1. Open a browser.
2. Type the following URL: **https://<ServicePortalAddress>/swagger-ui.html**
3. Log in with your user credentials.
4. The Swagger web interface for the Service Portal REST API opens.

### Using the Swagger web interface



**Asset Group API**  
/api-docs/Asset Groups

This API allows the management of tenant Asset Groups.

**Servers**  
https://10.10.244.107 - Generated server url

**v1 API Version 1**

- GET** /api/tenant/{tenant-id}/asset-group List the asset groups
- PUT** /api/v1/tenant/{tenant-id}/asset-group create or update asset
- GET** /api/v1/tenant/{tenant-id}/asset-group/{asset-group} Read an asset group
- DELETE** /api/v1/tenant/{tenant-id}/asset-group/{asset-group} Delete an existing asset group

**v2 API Version 2**

- GET** /api/v2/tenant/{tenant-id}/asset-group/{asset-group-id} Read an asset group
- PUT** /api/v2/tenant/{tenant-id}/asset-group/{asset-group-id} Update an existing asset group
- DELETE** /api/v2/tenant/{tenant-id}/asset-group/{asset-group-id} Delete an existing asset group
- GET** /api/v2/tenant/{tenant-id}/asset-group List the asset groups
- POST** /api/v2/tenant/{tenant-id}/asset-group Create a new asset group

**Schemas**

When you first open the Swagger web interface, you are in the first category of REST API operations: **Asset Group API**. Use the drop-down **(1)** at the top of the screen to navigate between categories.

To view a set of operations within a category, click the required version number **(2)**. To expand a single operation in a set, click on the operation title **(3)**.

Within each operation you can view the API model, an example value, the necessary parameters, and a list of possible response messages.

Within the Swagger interface, you can perform the operation by clicking **Try it out**, filling in any applicable parameter values and clicking **Execute**.

#### Tips for using Swagger:

- For PUT or POST operations where you require a body, use the **Example Value** prepopulated in the body field. You can then replace the placeholder strings with your own values. This ensures the body is formatted correctly.
- Swagger does not stop you entering invalid values in parameters (for example, a string value in a field expecting a number value). You will see an error when you perform the operation.
- If the response body contains a long message, it can be truncated. To see the full message, [run the same operation in cURL](#).
- Once you perform an operation, you will also see a cURL example of the same command.

**Caution:** Swagger does not correctly escape some special characters in the example cURL commands. You may need to edit the example cURL commands before using them.

## Using the REST API

You can use any tool, that enables you to send http requests to a URL, to interact with the Service Portal REST API. For example, cURL, the UNIX/Linux command line tool, or Postman.

### Available operations

The REST API supports tenant creation and management (including assets and tenant administrators). You cannot use the REST API to manage tenant users or to administer the Service Portal itself.

The Service Portal REST API supports the following HTTP operations:

- **GET** – Retrieves and displays information about a known resource or list of resources
- **POST** – Creates a new resource
- **PUT** – Edits an existing resource
- **DELETE** – Removes a known resource

You can use the methods above to perform operations in the following areas:

- Managing assets for tenants
  - Look up information on one or all assets
  - Create individual or multiple assets
  - Create, edit and delete asset groups
  - Edit assets: create asset names and assign to asset groups
  - Delete assets
- Managing tenants
  - Look up information on one or all tenants
  - Create individual or multiple tenants
  - Edit tenants: edit tenant details, modify applied service policy, enable/disable tenants, etc
  - Manage tenant administrators
  - Delete tenants
- Retrieving traffic and attack data for use with a custom front-end application

### Using Service Portal data to populate an existing front-end application

There are two REST API methods available if you need to get traffic and attack data from the Service Portal for your own custom front-end application. Using these methods, you can receive the information required to build graphs of inbound traffic and lists of attacks for each tenant.

- GET attacks – Gets a list of attacks for the tenant filtered according to one or more of the following parameters:
  - Start time (required)
  - End time ( if left blank, current time used)
  - DIP address, range or CIDR (if left blank, all tenant DIPs used)
- GET traffic – Gets a list of traffic data points for the tenant filtered according to one or more of the following parameters:
  - Start time (required)
  - End time ( if left blank, current time used)
  - DIP address, range or CIDR (if left blank, all tenant DIPs used)

**Caution:** Start and end times cannot be negative or zero values. You should make sure the start time is within the data period stored by the Service Portal.

### HTTP return codes

The Service Portal REST API supports the following HTTP return codes:

Code	Message	Description
200	OK	Your request was completed successfully and a response is returned.
201	Created	Your requested resource was created. The new resource URI is returned in the "Location" header.
202	Accepted	Your request was accepted, but has not been executed (and may not be executed).
204	No Content	Your request was completed successfully but there is no response to return.
400	Bad Request	Your request could not be processed because it contains missing or invalid information (for example a validation error on an input field or a missing required value).
401	Authentication Failed	Your request could not be processed because you weren't successfully authenticated.
403	Forbidden	You cannot access this resource with the credentials given.
404	Not Found	The resource you requested does not exist.

**Tip:** After you send a request, if you see the HTTP return code "204 No Content", that doesn't mean your request has failed - just that the Service Portal does not have anything to return after success.

## Versions

When you view the list of operations in Swagger, you can see the API version number in the path (e.g. /api/**v2**/tenant/{tenant-id}/assigned-asset).

When a new version of the API is released, the old version will be supported at least for the next release. The current version of the REST API is **v3**.

**Tip:** You can see all allowable operations for each API version in the Swagger REST API documentation.

## Etags

Versions v2 and v3 of the Service Portal REST API support the use of Etags.



This returns the details of the tenant who has that IP address in their Assigned Asset list. Those details include a ServicePolicyId which corresponds to one of your configured service levels.

To view the name and maximum mitigation for that ID, send the following request:

```
curl -k -u admin@admin.com:Admin123 -X GET --header 'Accept: application/json'
'https://<portal_IP>/api/v2/service-policy/<ID_number>'
```

## Troubleshooting

You are using an online-abridged copy of this user guide. For troubleshooting methods around managing local users and the appearance of traffic graphs, [contact your support representative](#) for a copy of the full **Corero SmartWall Service Portal User Guide**.



# Contacting Corero Customer Support

Corero Network Security offers two options for contacting Customer Services and Support.

- Contact the Customer Services Center by phone at + 1 978-212-1500
  - Support is available for all customers with a Hardware or Software Warranty from 8:00 AM to 5:00 PM (Eastern US Time).
  - If you have purchased the SecureWatch Managed Service, you can obtain service 24x7 by calling the support phone number and pressing Option 2. If the issue is critical, press Option 2 then Option 7.

**Note:** If, for any reason, the primary support phone number does not work, call Corero's answering service at +1.888.324.1246 (US) or +1.603.645.4145 (International) and a support representative will return your call.

- On the web through the Customer Support Portal: <https://corero.force.com/support/login/>. The Web Portal is the most effective way to log and track support issues. This Portal provides:
  - Web-based incident management and customer support tracking system
  - Service request communications
  - Access to downloadable files including software and product documentation
  - An extensive knowledge base.

When you contact Customer Services and Support for assistance, have the following information ready:

- The case number, if you are calling about a previous problem
- Your name, and if someone else will be the contact person for the problem, the contact person's name.
- Your company name and location (city, state or province, and country)
- The telephone number (including area code) at which you or the contact person can be reached.
- The email address at which you or the contact person can be reached.
- The product name, model number, and serial number.
- A list of system hardware and software, including revision levels.
- A detailed problem description:
  - Describe the symptom and the activities that preceded it.
  - Include details about any recent configuration changes, if applicable.
  - Be as specific as possible.
- Briefly describe your trouble-shooting steps and observations.

## Commenting on This Help Set

At Corero Network Security, our goal is to provide the highest quality products and services to our customers. We value customer feedback and encourage users of Corero's systems to send their comments on the product, service, and documentation to our Customer Service Department, so that we can continue to improve our products. Please send your comments and suggestions to Corero customer service at this email address: [customer.service@corero.com](mailto:customer.service@corero.com)

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://corero.force.com/support>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://apex.juniper.net/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

## Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://apex.juniper.net/>
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

## Requesting Licenses

The system requires a TDD license key, plus keys for each vNTD, to become fully operational. Juniper devices do not require license keys to support the solution. To obtain the keys, please contact the Corero Customer Services team by one of the following methods:

- Email: [Support.Portal@corero.com](mailto:Support.Portal@corero.com)
- Web: <https://corero.force.com/support>
- Telephone: Dial +1.978.212.1500 -> Select Option 2