



Corero Network Security

SmartWall Service Portal User Guide

Software Version 1.2.3

13 April 2020

Part Number: 9302-0123-00-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.

Copyright © 2014- 2020, Corero Network Security, Inc.

CONTENTS

Legal and Copyright Information	2
Contents	3
SmartWall Service Portal	9
Corero Concepts	10
SmartWall System	10
Sample-based traffic information	11
Tenants	11
Assets	11
Working in the Service Portal	11
Getting Started	12
Hardware Requirements for Installation	13
Minimum system requirements	13
Recommended system requirements	13
Installing the Service Portal	14
Configuring the SWA to Forward Data to the Service Portal	15
Forward traffic from a 9.7.2 SWA	15
Forward traffic and attack information from 9.7.0 and earlier SWA's	16
Upgrading the Service Portal	18
Logging In to the Service Portal	19
To log in to the Service Portal	19
To log out of the Service Portal	19
Tuning your Sample Rate	19
Changing your own Password	20

CONTENTS

To change your password from inside the Service Portal	20
To recover your password using email verification	20
Editing your own User Profile	21
To edit your user profile	21
Configure the Service Portal	22
Users Overview	23
LDAP Authentication	23
Users Settings Screen	24
LDAP Settings Screen	26
Managing Users	29
Configuring LDAP Integration for Authentication Users	30
User Audit Log	33
Audit Settings Screen	33
Exporting the Audit Log	35
To export the Audit Log	35
Managing Audit Log Rotation	35
To manage Audit Log rotation	35
Service Policy and Alerting	36
Service Levels	36
Alerts	37
Policy Settings Screen	40
Configuring Service Levels	41
Scheduled Reporting	42
Report emails	42
Reporting Settings Screen	44

CONTENTS

Managing Scheduled Reporting	45
Licensing	47
Licensing Settings Screen	47
Adding a license to the Service Portal	49
Logo	50
Logo Settings Screen	50
Adding a Logo to the Service Portal	51
Password Expiry Options	52
Password warning and grace periods	52
Per-Tenant password expiry options	52
Password Settings Screen	52
Managing Password Expiry Options	54
Usage Statistics	56
Usage Settings Screen	56
Diagnostics	58
Diagnostic Settings Screen	58
Download Diagnostics to Investigate an Issue	59
Tenants Overview	60
Tenant traffic and attacks	60
Assets	61
Reassigning an Asset	62
Tenant user roles	62
Tenant Management screen	62
Create a tenant	63
Find a tenant	63

CONTENTS

Navigate a Tenant's options	63
Creating a New Tenant	65
Prerequisites	65
To create a new tenant	65
Next Steps	66
Importing Multiple Tenants	67
To import multiple tenants	67
Next steps	68
Managing a Tenant's Users	69
To add a new user	69
Managing a Tenant's Assets	70
To add a new Assigned Asset	70
To add a new Named Asset	70
To create an asset group	71
Importing Multiple Assets	72
Prerequisites	72
To import multiple assets	72
Viewing Tenant Attacks	74
Prerequisites	74
To view a tenant's dashboard	74
Changing a Tenant Name and Description	76
To change a tenant's name	76
To change a tenant's description	76
Changing a Tenant Service Level	76
To change a tenant's service level	76

CONTENTS

Editing a Tenant's Primary Contact Information	77
To edit a tenant's primary contact information	77
Enabling/disabling a Tenancy	78
To enable or disable a tenancy	78
Deleting a Tenant	78
To delete an existing tenant	78
Service Overview and Attack Analysis	79
Print attack reports	79
Service Overview screen	80
Filters	80
Attack Analysis screen	83
Traffic considerations for Service Portals connected to a SmartWall TDD system	85
Differences between the Service Portal and SmartWall TDD attack charts	85
Common Analysis Tasks	86
To view any ongoing attacks in your network	86
To view the tenants who experience the most attacks today	86
To view the most attacked IP addresses in the past week	86
To view all attacks against a single tenant	86
To view all attacks between two dates	87
To view all attacks against a tenant in the past day	87
To print a report showing all attacks against an IP address in the last week	87
Service Portal REST API Overview	88
Accessing the REST API documentation	88

CONTENTS

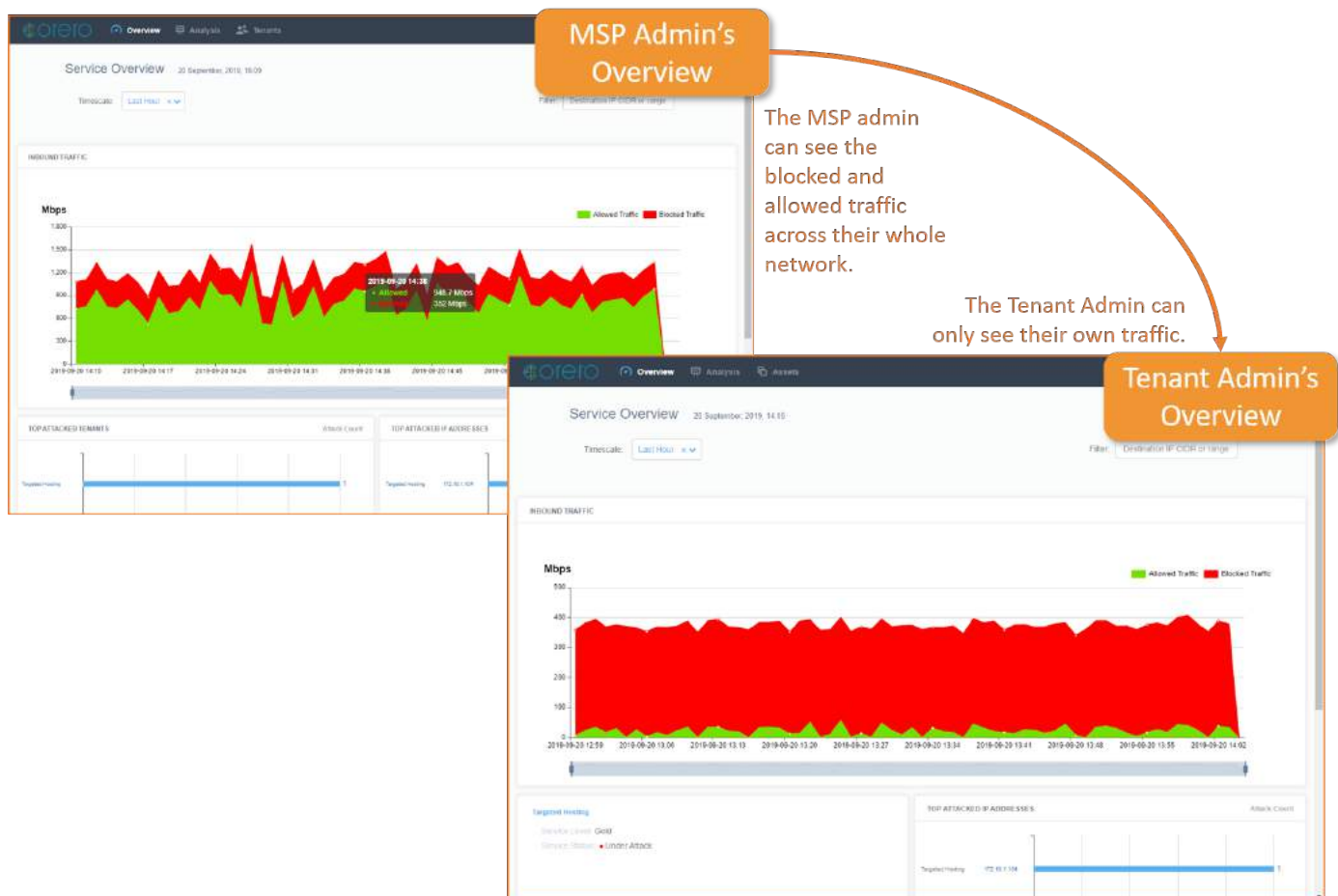
Using the Swagger web interface	88
Using the REST API	89
Available operations	89
HTML return codes	90
Versions	91
Etags	91
Using cURL	91
Troubleshooting	93
Appendix: Using a Remote Database	94
Requesting Technical Support	95
Self-Help Online Tools and Resources	95
Creating a Service Request with JTAC	95
Requesting Licenses	96

SmartWall Service Portal

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

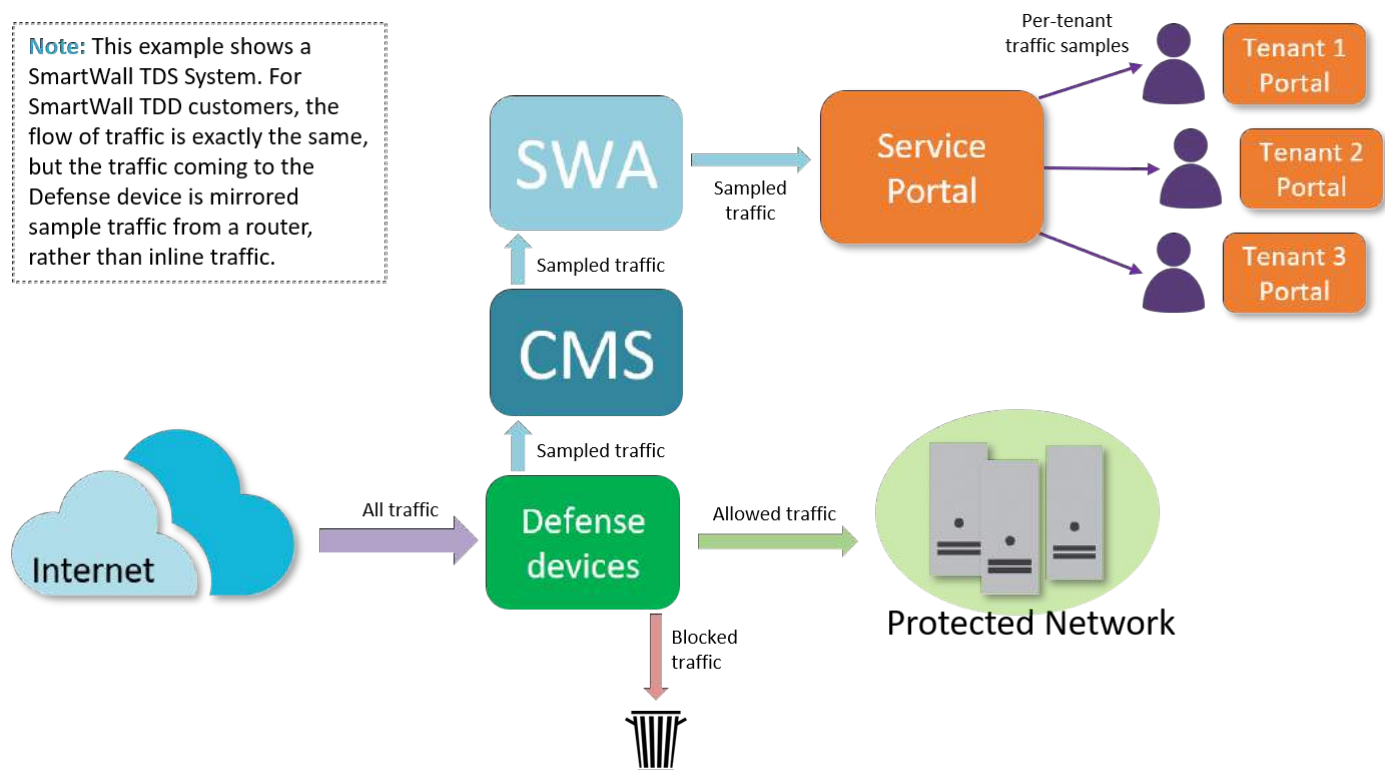
The Service Portal uses sampled traffic data from your SmartWall Threat Defense System (SmartWall TDS) or SmartWall Threat Defense Director (SmartWall TDD). It displays the information in easy to read charts and reports. You can create reports for your customers to highlight the value they receive from 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

Note: This example shows a SmartWall TDS System. For SmartWall TDD customers, the flow of traffic is exactly the same, but the traffic coming to the Defense device is mirrored sample traffic from a router, rather than inline traffic.



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:** 64 or newer
- **Internet Explorer:** 11 or newer
- **Edge:** 40 or newer
- **Firefox:** 58 or newer
- **Safari:** 11 or newer

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](#).

Hardware Requirements for Installation

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

Minimum system requirements

The following requirements are necessary for a functional Service Portal:

- 4 vCores
- 16GB RAM
- 200GB 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)

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.

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**.

Configuring the SWA to Forward Data to the Service Portal

To see your network's traffic information in the SmartWall Service Portal, you need to feed the metadata from sampled traffic from your SmartWall SecureWatch Analytics (SWA) application. SWA is the analytics application in the SmartWall Threat Defense System which stores and organizes your networks traffic information.

The sample traffic is sent over UDP on port 5410.

Note: The following method is for SmartWall SecureWatch Analytics Virtual Edition (vSWA). 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.

Forward traffic from a 9.7.2 SWA

Prerequisites

You must have the following:

- A Service Portal running version 1.2 or later

To connect a 9.7.2 SWA application to a Service Portal

1. Open the SWA in a browser and log in.
2. Use the top menu to navigate to **System > Service Portal Configuration**.
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.
 - c. The default **Syslog Port** is **5410**.
4. To enable syncing of Service Levels between the SWA and the Service Portal:
 - a. Under **Enable SSP synchronization**, click the grey slider. It will turn green to show syncing is enabled.
 - b. Type the **Username** for an MSP Administrator account in the Service Portal.
 - c. Type the corresponding **Password** for that account.
 - d. The default **REST API Port** is **443**.
 - e. Enable the SWA to keep up to date with the Service Portal, by polling for changes every minute. Under **Enable Periodic Sync**, click the grey slider. It will turn green to show syncing is enabled.
5. Click **Save**.
6. (Optional) To immediately sync Service Levels to your SWA from the Service Portal, click **Sync Now**. You will see a message appear above the button to show how many changes were brought over.

Forward traffic and attack information from 9.7.0 and earlier SWA's

Prerequisites

Before you begin, you need an operational vSWA application, to which you have administrative access and an operational Service Portal.

You must know the following information:

- *<swaUsername>* – The username of the SWA administrative user account. You must also know the corresponding password. If you did not change the default SWA credentials after deployment, this will be admin/smartwall.
- *<swaIPAddress>* – The IP address of the SWA application.
- *<ServicePortalIP>* – The IP address of the Service Portal.

To configure a 9.7.0 or earlier vSWA application to forward data to the Service Portal

1. Open a console session to the vSWA and log in with the admin account. If you're using an ssh client, type the following command then when prompted enter your password: `ssh -p 2222 <swaUsername>@<swaIPaddress>`

2. Type the following command:

```
setup service-portal
```

3. The setup wizard enables you to configure the connection to the Service Portal. The recommended commands are in *italics*; where there is no command, press the return key to accept the default value. You must also replace any placeholders with your system information:

```
Please configure the Service Portal connection:
```

```
Enable sending data to the Service Portal? <Y, [N]>: y
```

```
Enter IP Address [None]: <ServicePortalIP>
```

```
Enter Port [5410]:
```

4. Once you press the return key to accept the default port, you'll see a summary of the Service Portal configuration:

```
Service Portal:
```

```
State : Enabled
```

```
IP Address : <ServicePortalIP>
```

```
Port : 5410
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]:
```

5. If you're happy, press the *A* key, or press the *C* key to change any of those details.
6. To confirm setup was successful, once the changes have been applied type the following command:

```
setup service-portal
```

7. You will see the following, note that the **State** is now "Enabled":

```
Please configure the Service Portal connection:
```

```
Enable sending data to the Service Portal? <[Y], N>: y
```

```
Service Portal:
```

```
State : Enabled
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]:
```

8. Press the *E* key to exit setup without changing anything.
9. Open the Service Portal in a browser (<https://<ServicePortalIP>:8080>) and check you can see traffic on the System Overview screen.

Upgrading the Service Portal

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

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](#).

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

To log in to the Service Portal

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

To log out of the Service Portal

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

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 emails by checking the boxes next to any of the following:
 - **Service level status alerts**
 - **Attack status alerts**
 - **Service overview reports**
 - **Per tenant reports**
5. Click **Save**.

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

Configure the Service Portal

Note: Configuring the Service Portal must be performed by an MSP Administrator. If you are an MSP User, you can only [view policy information](#); you can skip to [Tenants](#) 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.

Users Overview

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.

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.

System Settings

Toolbar

Users | LDAP | Audit | Policy | Reporting | Licensing | Logo | Password | Usage | Diagnostics

Filters

☒ MSP Roles ☒ Tenant Roles [Create User](#)

Username/Email	First Name	Last Name	Phone	Status	Timezone	Last Login	Role	Tenant	Authentication	Actions
admin@admin.com	MSP	ADMIN	+44	Enabled	UTC+01:00	2019-09-20 15:09	MSP Administrator	N/A	Internal	Edit
test@test.com	test	test.com		Enabled	UTC+00:00	2019-09-17 00:54	Tenant Administrator	Targeted Hosting	Internal	Edit Delete
tenant@admin.com	Test	User		Enabled	UTC+00:00	2019-09-20 14:58	Tenant Administrator	Targeted Hosting	Internal	Edit Delete



1 - 3 of 3 results [Show](#)

Copyright © 2019 Corero SmartMail® Service Portal v1.2.0 (2020) 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:

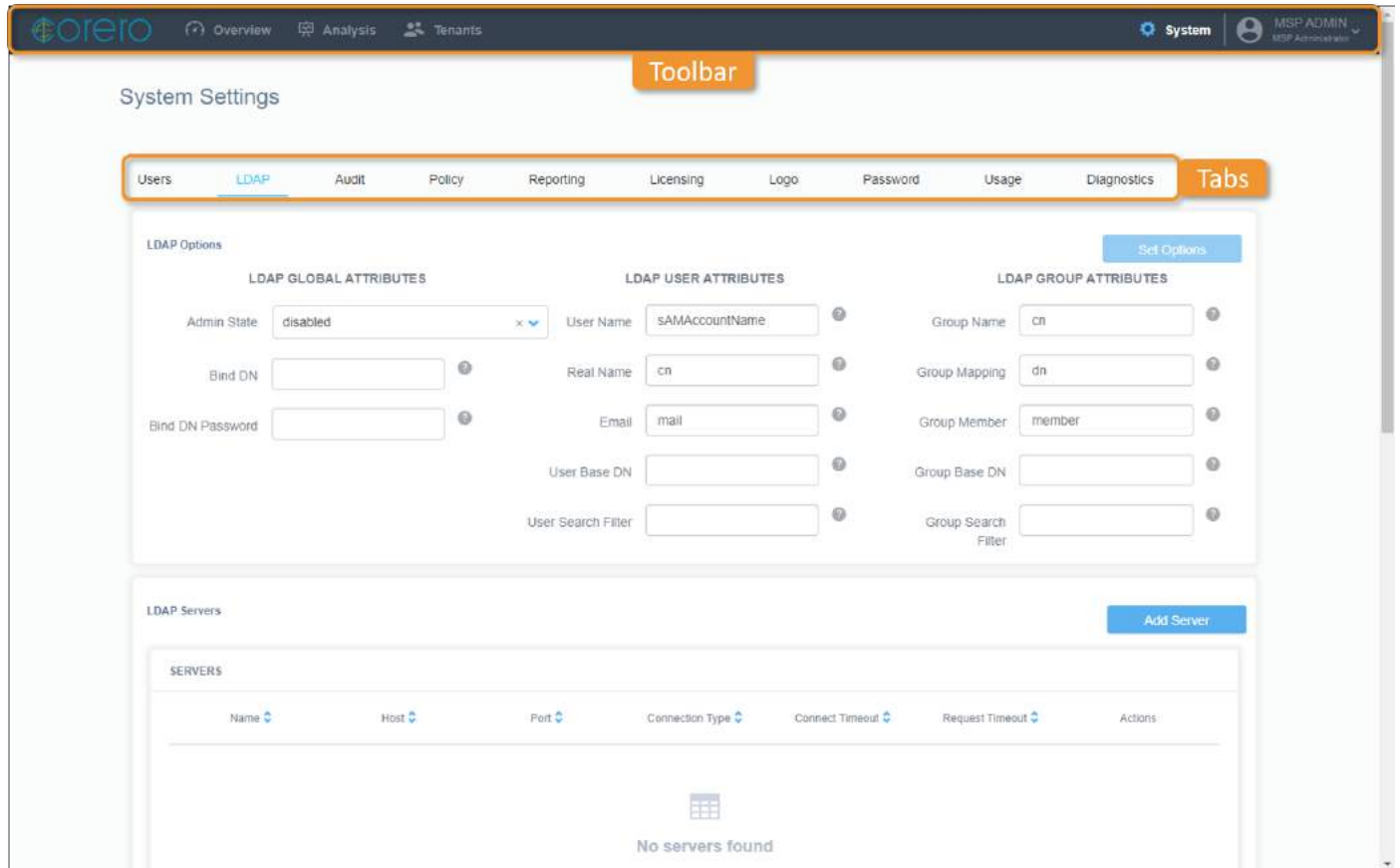
- **Username/Email** – Select this option then type all or part of an email address to view only users whose email address matches the search term. For example, you can filter to only show users who use company email addresses by typing the last half of an email (i.e. @company.com).
- **First Name** – 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.





The screenshot shows the Corero System Settings interface. At the top, there's a toolbar with 'System' selected. Below it, the 'System Settings' section has tabs for 'Users', 'LDAP', 'Audit', 'Policy', 'Reporting', 'Licensing', 'Logs', 'Password', 'Usage', and 'Diagnostics'. The 'LDAP' tab is active. It contains three main sections: 'LDAP GLOBAL ATTRIBUTES', 'LDAP USER ATTRIBUTES', and 'LDAP GROUP ATTRIBUTES'. Each section has several input fields and a 'Set Options' button. Below these is the 'LDAP Servers' section, which has an 'Add Server' button and a table with columns: Name, Host, Port, Connection Type, Connect Timeout, Request Timeout, and Actions. The table is currently empty, showing 'No servers found'.

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.

- 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

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

1. From the main toolbar of the Service Portal, click **System**. 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.
 - **Password** – Type a password for this user. They will be able to change this later.
 - **Confirm Password** – Re-type the password.
 - **Phone** – (Optional) Type in a contact telephone number for the user
 - **Timezone** – From the drop-down, select the timezone this user is normally based in
 - **Suppress Emails** – Select any of the check boxes to stop the user receiving emails about specific alerts or reports.
4. Click **Save**.

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

Configuring LDAP Integration for Authentication Users

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**. 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. 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
5. 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
6. Click **Set Options**.

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**.

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.

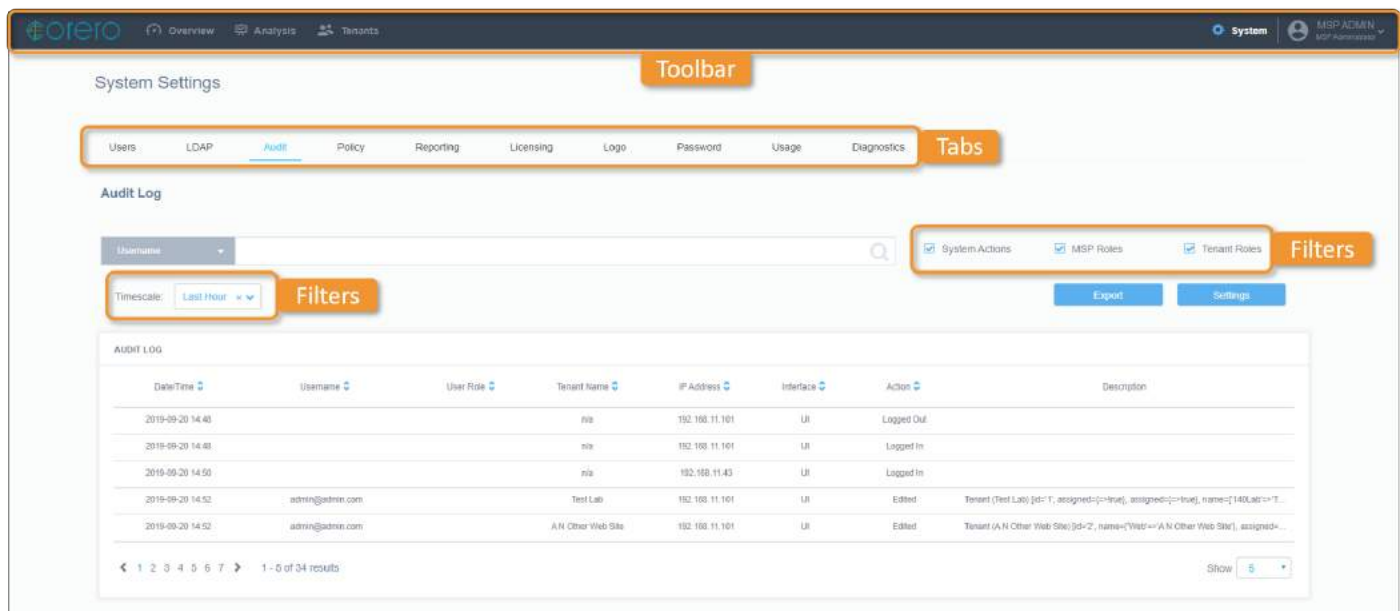
What you see on the audit log depends on your User Role:

- 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** on the main toolbar then the **Audit** tab.



System Settings

Toolbar

Users | LDAP | **Audit** | Policy | Reporting | Licensing | Logo | Password | Usage | Diagnostics

Audit Log

Username:

Timescale: **Last Hour**

☒ System Actions ☒ MSP Roles ☒ Tenant Roles

DateTime	Username	User Role	Tenant Name	IP Address	Interface	Action	Description
2019-09-20 14:40			n/a	192.168.11.101	UI	Logged Out	
2019-09-20 14:40			n/a	192.168.11.101	UI	Logged In	
2019-09-20 14:50			n/a	192.168.11.43	UI	Logged In	
2019-09-20 14:52	admin@admin.com		Test Lab	192.168.11.101	UI	Edited	Tenant (Test Lab) [id=1, assigned=<=>true], assigned=<=>true, name=<=>1403,ac=<=>T...
2019-09-20 14:52	admin@admin.com		A/N Other Web Site	192.168.11.101	UI	Edited	Tenant (A/N Other Web Site) [id=2, name=<=>Web=<=>A/N Other Web Site], assigned=<=>...

1 - 5 of 34 results 5

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**.
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**.
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**.

Service Policy and Alerting

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

The Service Portal can send email notifications to users when an event occurs which they may need to be aware of. For every service level, you can choose to configure 2 alert types:

- **Service level alerts** – The Service Portal sends an email to the selected recipients when a tenant exceeds this service level's maximum mitigation rate.
- **Attack status alerts** – The Service Portal sends an email 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).

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 email subject and body. In the email subject and body, you can include placeholder fields; these instruct the Service Portal to insert changeable information before it sends the email. 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.

- **{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 is 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
- **{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.

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}**.

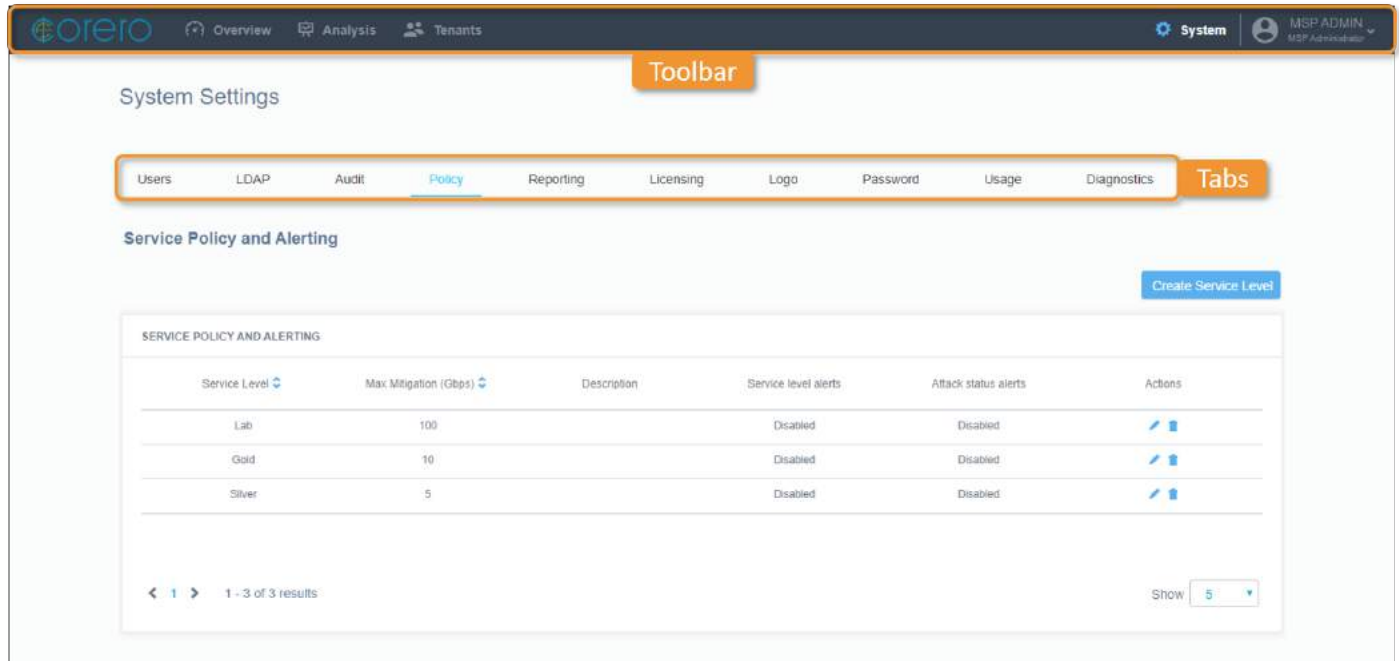
The following is a summary of the attack:

{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}**

Policy Settings Screen

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









System Settings

Toolbar

Tabs

Service Policy and Alerting

[Create Service Level](#)



Service Level	Max Mitigation (Gbps)	Description	Service level alerts	Attack status alerts	Actions
Lab	100		Disabled	Disabled	 
Gold	10		Disabled	Disabled	 
Silver	5		Disabled	Disabled	 

1 - 3 of 3 results

Show 5

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
-  – 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.

Configuring Service Levels


Once you chose a subscription structure for your tenants, you'll need to configure the SmartWall Service Portal's policy to reflect the 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 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

1. From the main toolbar of the Service Portal, click **System**, 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. If you want users to be alerted when a tenant exceeds this service level's max mitigation rate, complete the following fields on the **Service level alerts** tab:
 - **Enable alerting** – By default alerting is **Disabled** for a new service level, to start using Service level alerts, select **Enabled**
 - **Subject** – Edit the example subject line for the service level 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.
 - **Email Body** – Edit the example contents of the service level 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 subject line. When the email is sent, the Service Portal populates the placeholder field with the relevant information.
 - **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, which has exceeded its max mitigation rate
 - **Tenant Users** – The Tenant Users for a tenancy, on this service level, which has exceeded its max mitigation rate

5. If you want users to be alerted when a tenant on this service level experiences an attack, complete the following fields on the **Attack status alerts** tab:
 - **Enable alerting** – By default alerting is **Disabled** for a new service level, to start using Attack status alerts, select **Enabled**
 - **Subject** – Edit the example subject line for the attack status 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.
 - **Email Body** – Edit the example contents of the attack status 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 subject line. When the email is sent, the Service Portal populates the placeholder field with the relevant information.
 - **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, which has experienced an attack
 - **Tenant Users** – The Tenant Users for a tenancy, on this service level, which has experienced an attack
6. When you're happy with your settings, click **Save**.

Note: You can edit  or delete  service levels from the Service Policy table.

Scheduled Reporting

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:

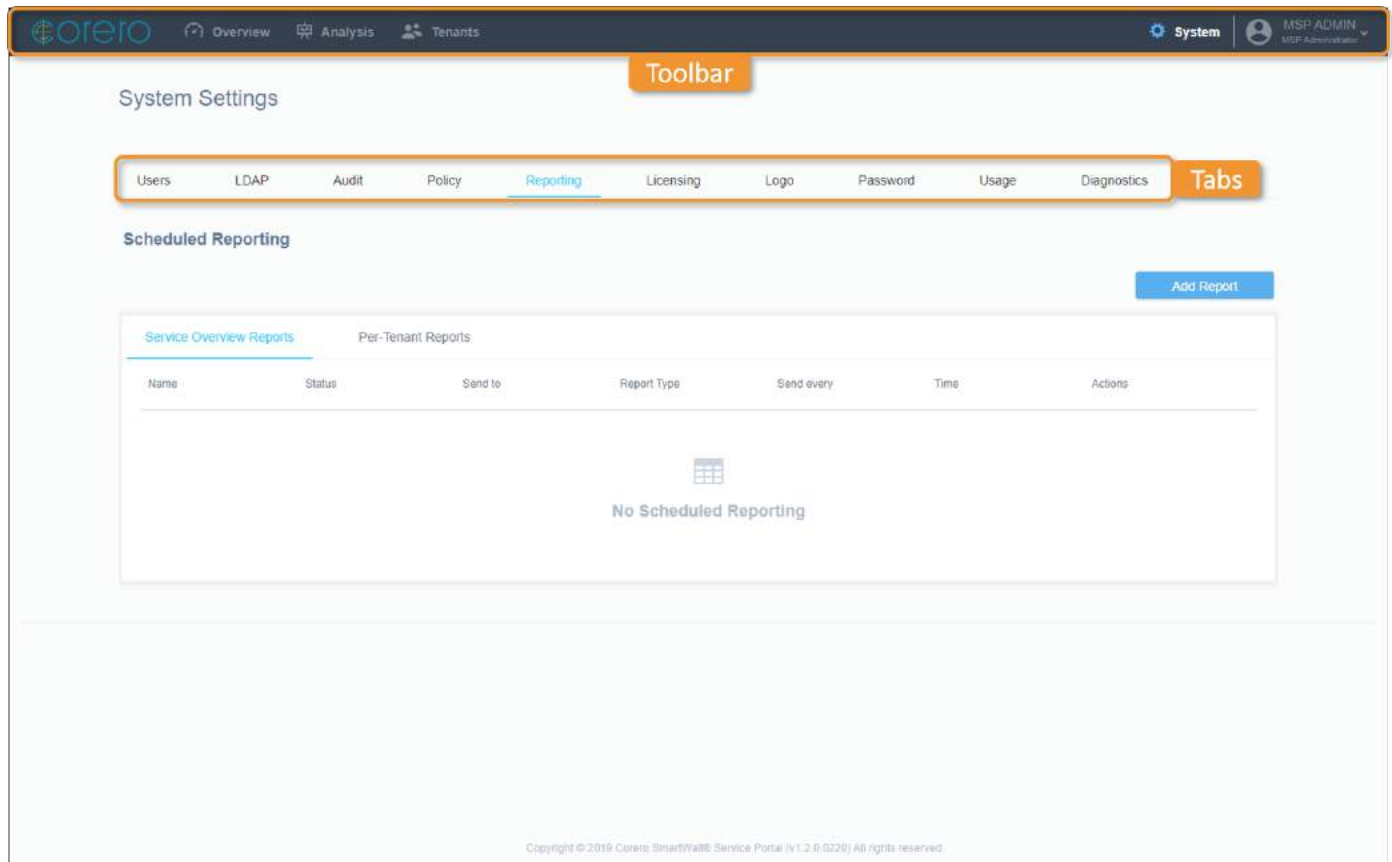
The attached report covers all mitigated DDoS attacks for **{tenant_name}** over the past **{report_time_duration}** **{report_time_period}**s.

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.

Reporting Settings Screen

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







The screenshot displays the Corero System Settings interface. At the top, the 'System' tab is selected in the main toolbar. Below it, the 'Reporting' tab is highlighted in the sub-navigation bar. The 'Scheduled Reporting' section is active, showing an 'Add Report' button. A table header is visible with columns: Name, Status, Send to, Report Type, Send every, Time, and Actions. The table body is empty, showing 'No Scheduled Reporting'.

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



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 Users**; all reports are sent to **MSP Admins** and **MSP 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.

Licensing

When you install the SmartWall SecureWatch Analytics 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 25 tenants.

When you're ready to upgrade to a full license, you need to contact your support representative. When you contact support, you need to quote your System UUID. This is visible on the licensing tab of the system settings screen. Your support representative will then provide you with a License Key that you need to enter on the Licensing page to remove the evaluation tenant limit.

Note: The license is specific to your System UUID and cannot be used on another Service Portal.

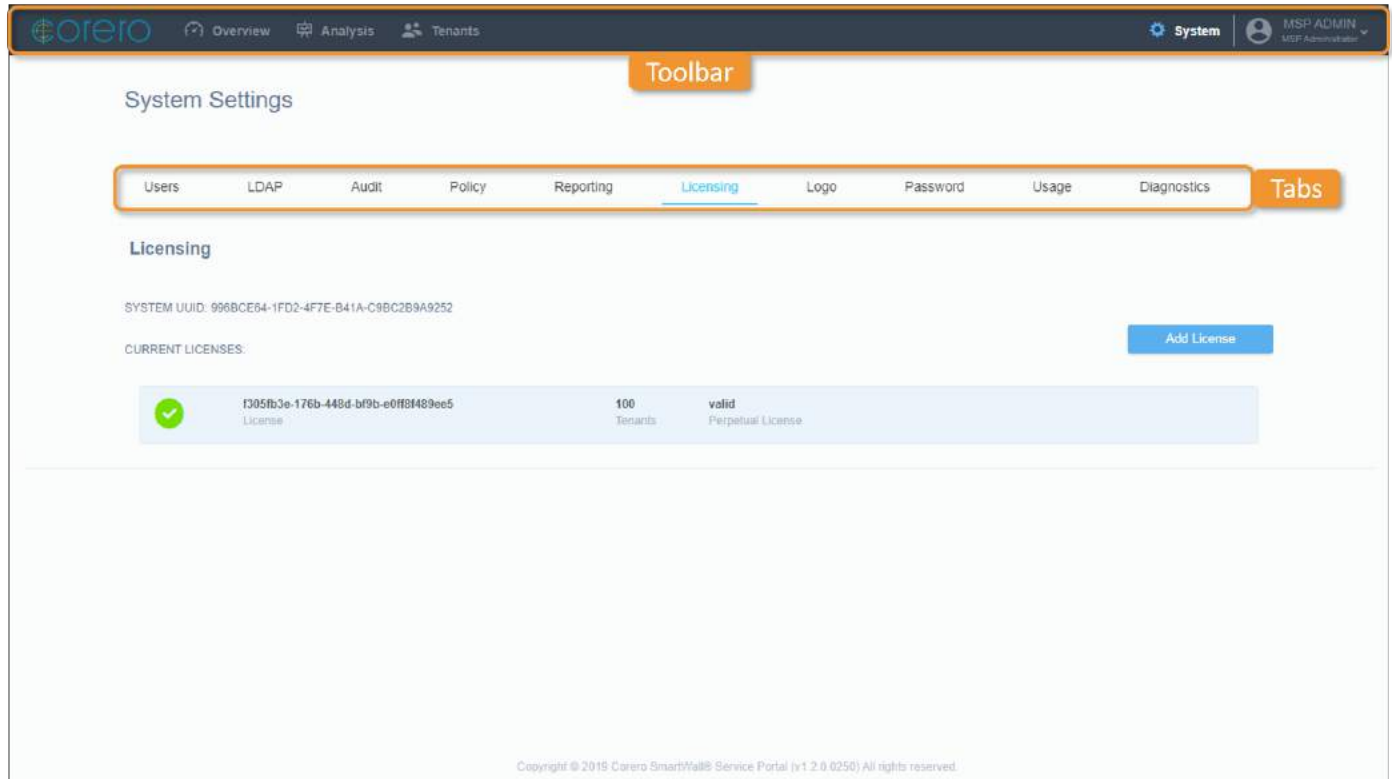
If your license has an expiry date, your support representative will make you aware of the following:

- 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.

Licensing Settings Screen

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



The screenshot shows the Corero System Settings interface. At the top, there is a navigation bar with 'Overview', 'Analysis', and 'Tenants' tabs. Below this is a 'System' settings bar with a gear icon and a user profile 'MSP ADMIN'. The main content area is titled 'System Settings' and features a 'Toolbar' with a 'Toolbox' button. Below the toolbar is a 'Tabs' section with options: Users, LDAP, Audit, Policy, Reporting, Licensing (selected), Logo, Password, Usage, and Diagnostics. The 'Licensing' section displays the 'SYSTEM UUID: 996BCE64-1FD2-4F7E-B41A-C9BC2B9A9252' and a list of 'CURRENT LICENSES'. A single license is shown with a green checkmark icon, the ID 'f305fb3e-176b-448d-bf9b-e0ff8f489ee5', '100 Tenants', and 'valid Perpetual License'. An 'Add License' button is located to the right of the license list. At the bottom, a copyright notice reads: 'Copyright © 2018 Corero SmartWall® Service Portal (v1.2.0 0250) All rights reserved.'

The current license show the following information:

- License – The name of your license.
- Tenants – The number of tenants you can have under this license.
- License status – The status is 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

When you install the SmartWall Service Portal you receive an evaluation license. When you are ready to enable a full license you need to enter your unique License Key.

Prerequisites

You need to contact your Corero representative for a License Key.

To add a license to the Service Portal

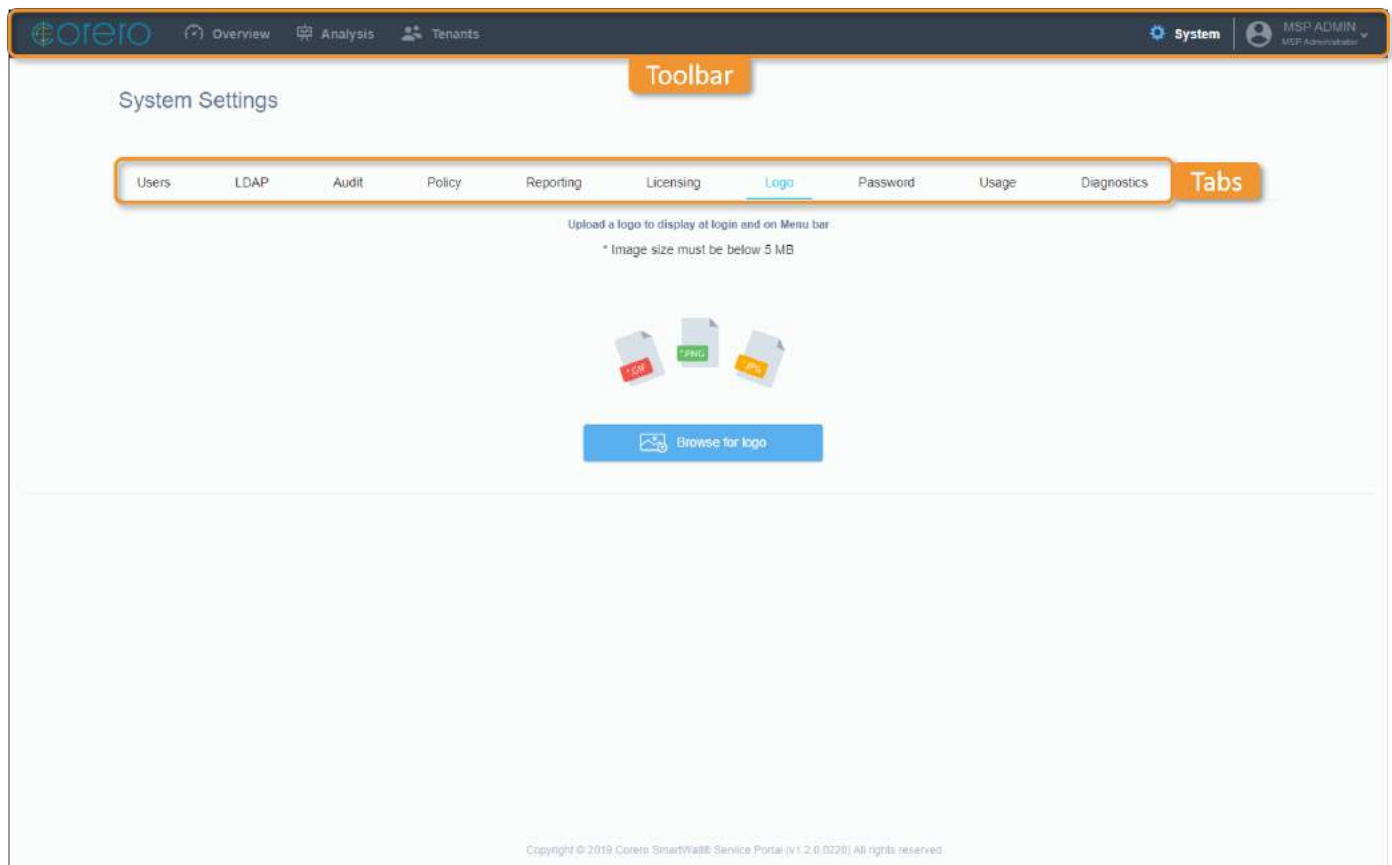
1. From the main toolbar of the Service Portal, click **System**, then the **Licensing** tab.
2. Click **Add License**.
3. In the field which appears, type the **License Key** provided by Corero.
4. Click **Confirm**.

Logo

Before you start adding tenants to the SmartWall Service Portal you should make sure the portal is branded for your organization. You can add a logo that appears on the log in 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.

Logo Settings Screen

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



The logo image must adhere to the following criteria:

- The file size must be less than 5 MB
- The file format must be PNG or JPG

Adding a Logo to the Service Portal

To customize the SmartWall Service Portal for you and your tenants you can add your organization's logo to the top left of the main toolbar and to the log in page.

To add a logo to the Service Portal

1. From the main toolbar of the Service Portal, click **System**, then the **Logo** tab.
2. Either drag and drop an image onto the center of the Logo tab, or click **Browse for logo** to select an image file from your computer.
3. Once the logo has successfully uploaded you should see it appear in main tool bar.

To update the logo at a later date, repeat the same process with your new image file.

Password Expiry Options

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.

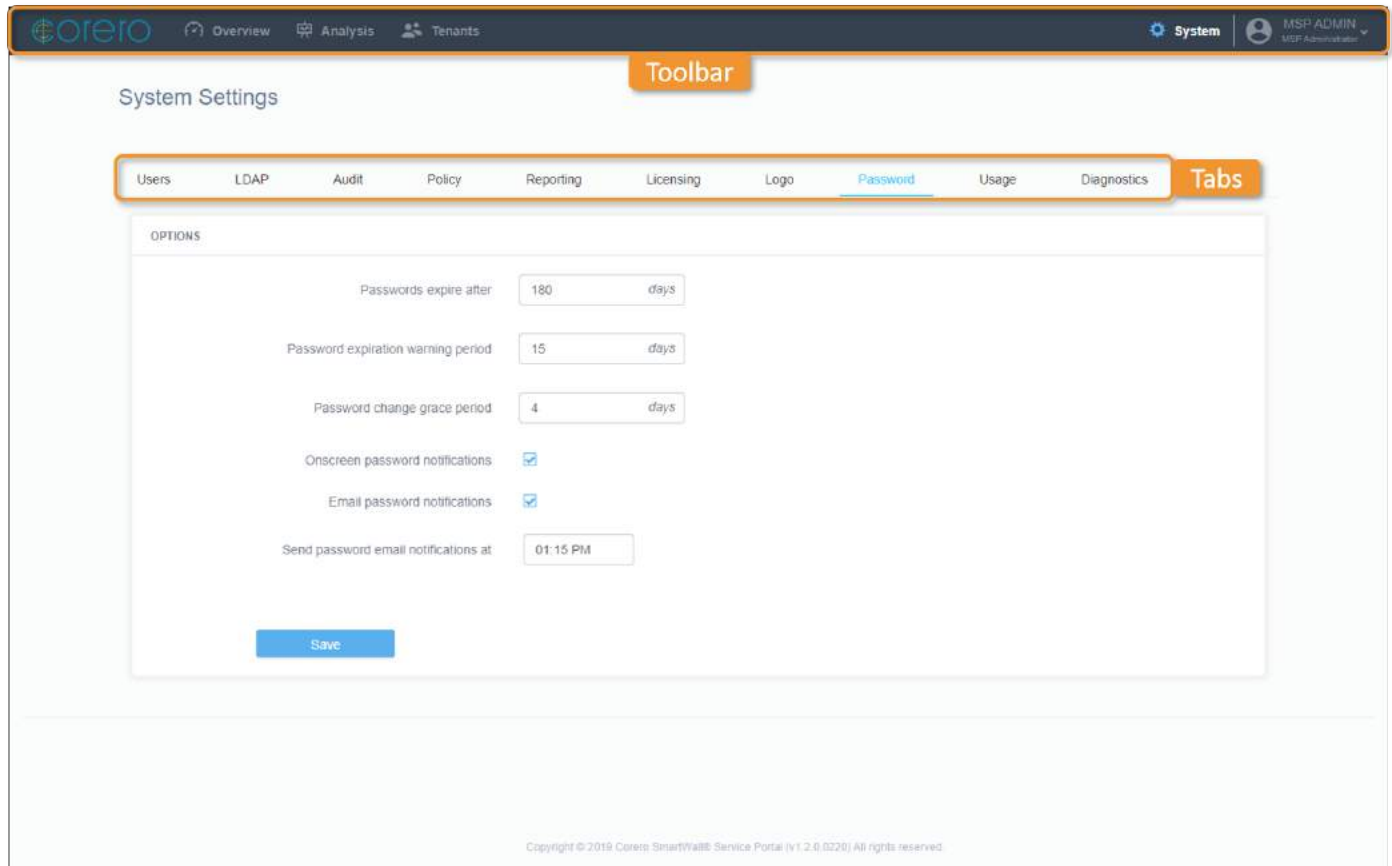
If a user does not change their password during the warning period or grace period, they must contact their administrator to have the password reset.

Per-Tenant password expiry options

You can override the system-wide password expiry options for specific tenants. When you select a tenant on the Tenant 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 Settings Screen

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



The screenshot shows the Corero System Settings interface. At the top, there's a navigation bar with 'Overview', 'Analysis', and 'Tenants' tabs. Below this is a 'System' section with a user profile 'MSP ADMIN'. The main content area is titled 'System Settings' and features a 'Toolbar' with various tabs: 'Users', 'LDAP', 'Audit', 'Policy', 'Reporting', 'Licensing', 'Logo', 'Password' (selected), 'Usage', and 'Diagnostics'. The 'Password' tab is active, showing a form with the following options:

- Passwords expire after:** 180 days
- Password expiration warning period:** 15 days
- Password change grace period:** 4 days
- Onscreen password notifications:** ☒
- Email password notifications:** ☒
- Send password email notifications at:** 01:15 PM

A 'Save' button is located at the bottom of the form. At the very bottom of the page, a copyright notice reads: 'Copyright © 2019 Corero SmartWall® Service Portal (v1.2.6.0228) 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.

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**, 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 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.
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**.

Usage Statistics

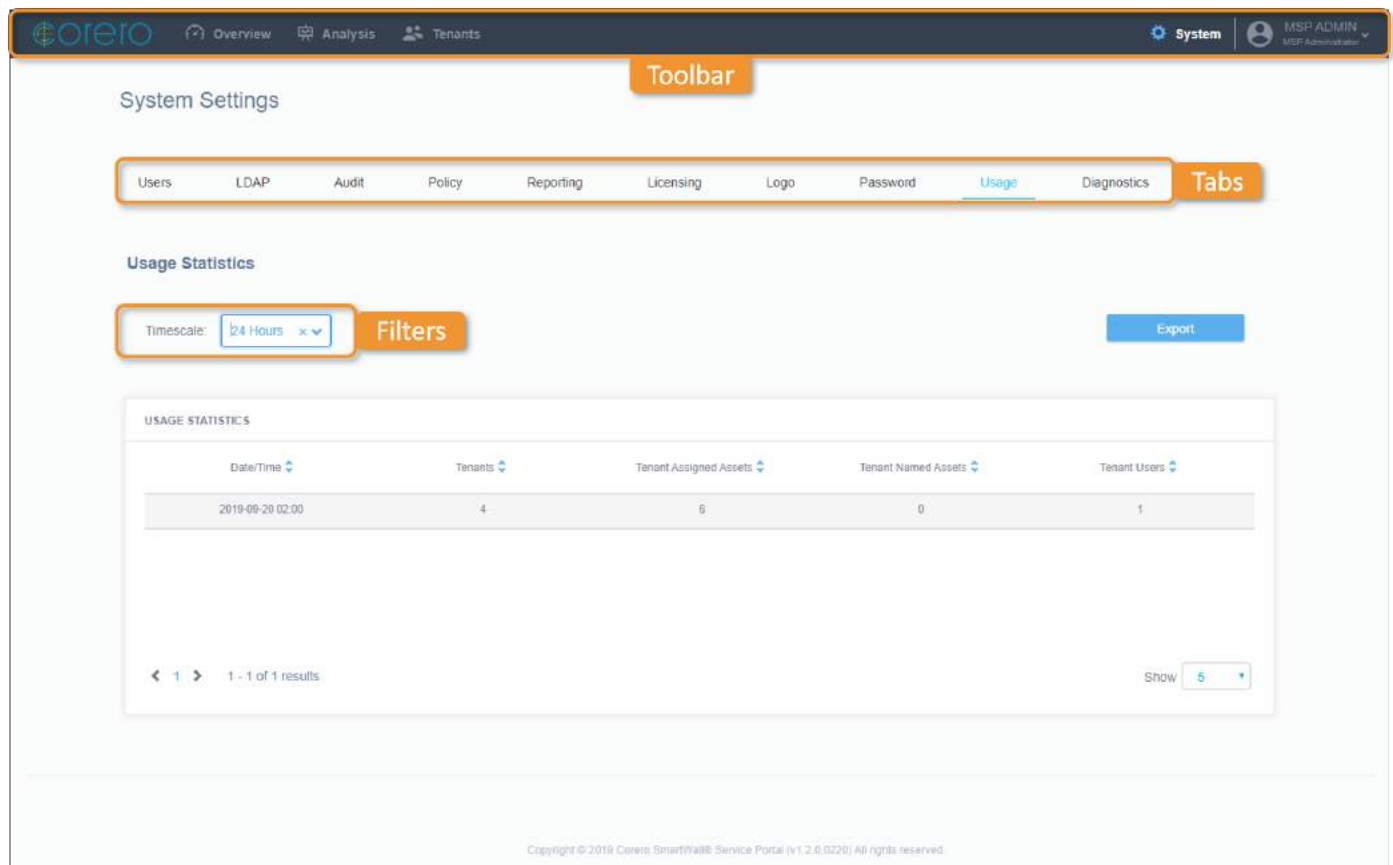
You can see how you're using the Service Portal in the Usage Statistics table. Every day the system checks how many tenants are enabled, how many assets have been assigned to all tenants, how many assets have been named, and how many tenant users there are.

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 Settings Screen

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



System Settings

Usage Statistics

Timescale: 24 Hours x Filters Export

Date/Time	Tenants	Tenant Assigned Assets	Tenant Named Assets	Tenant Users
2019-09-20 02:00	4	6	0	1

1 - 1 of 1 results Show 5

Copyright © 2019 Corero SmartWall® Service Portal (v1.2.0.0220) All rights reserved.

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

Diagnostics

The Service Portal contains data on actions, events, and other information which can be useful to review when trying to diagnose an issue with the Service Portal. If Corero Customer Support asks for a diagnostics file, you can download either:

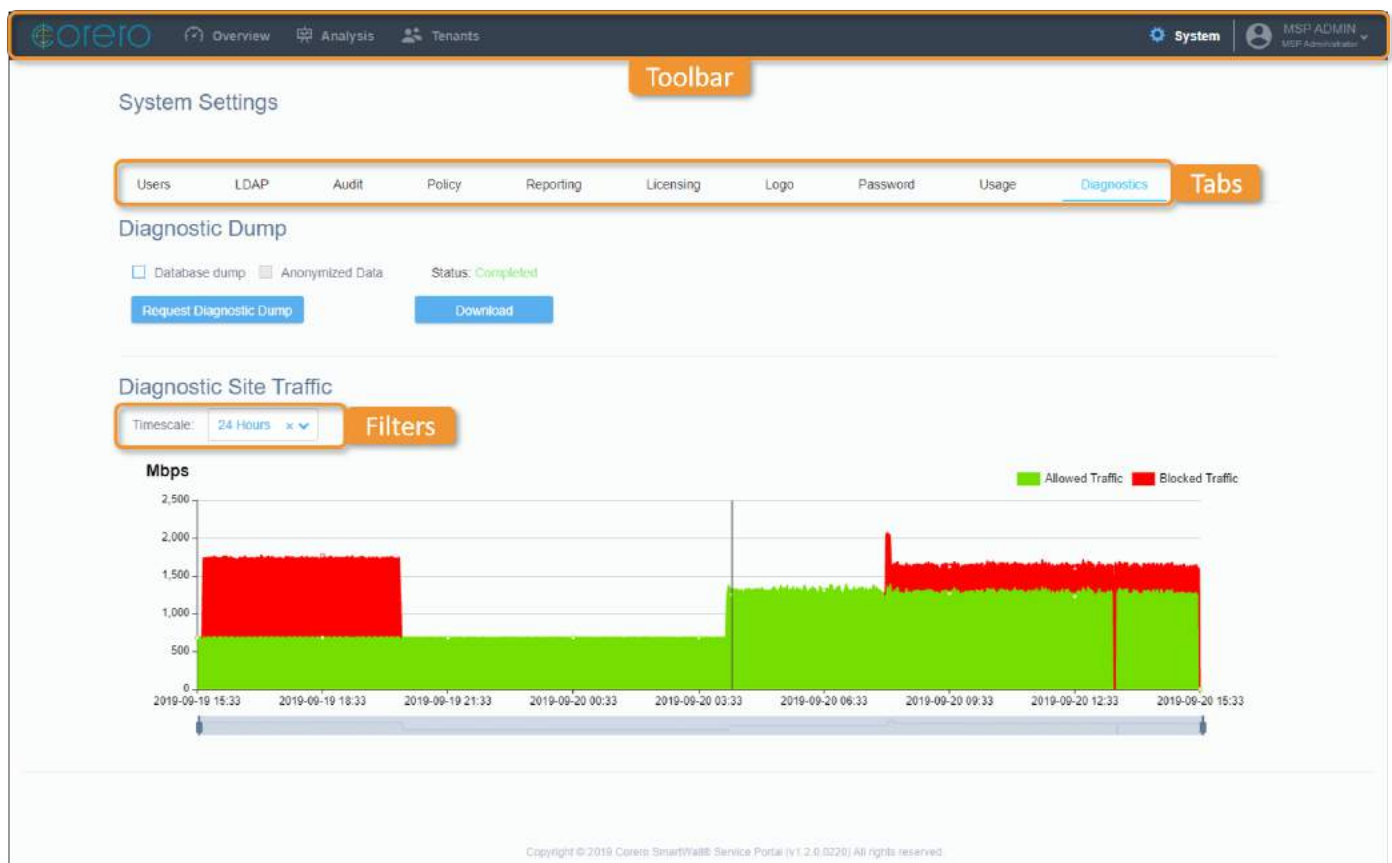
- The diagnostic files
- The diagnostic files and a database dump
- The diagnostic files and an anonymized database dump (where company and customer details are removed)

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

You can also view a chart of site traffic.

Diagnostic Settings Screen

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



The Diagnostic Site 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.

Download Diagnostics to Investigate an Issue

To assist Corero Customer Support or for your own investigations into an issue, you can download a set of diagnostic files which can optionally contain the information from the Service Portal database.

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

To download Service Portal diagnostics

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

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 amount of tenants you can have depends on your license. The smallest license allows for up to 25 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 tenants **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 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 tenants 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

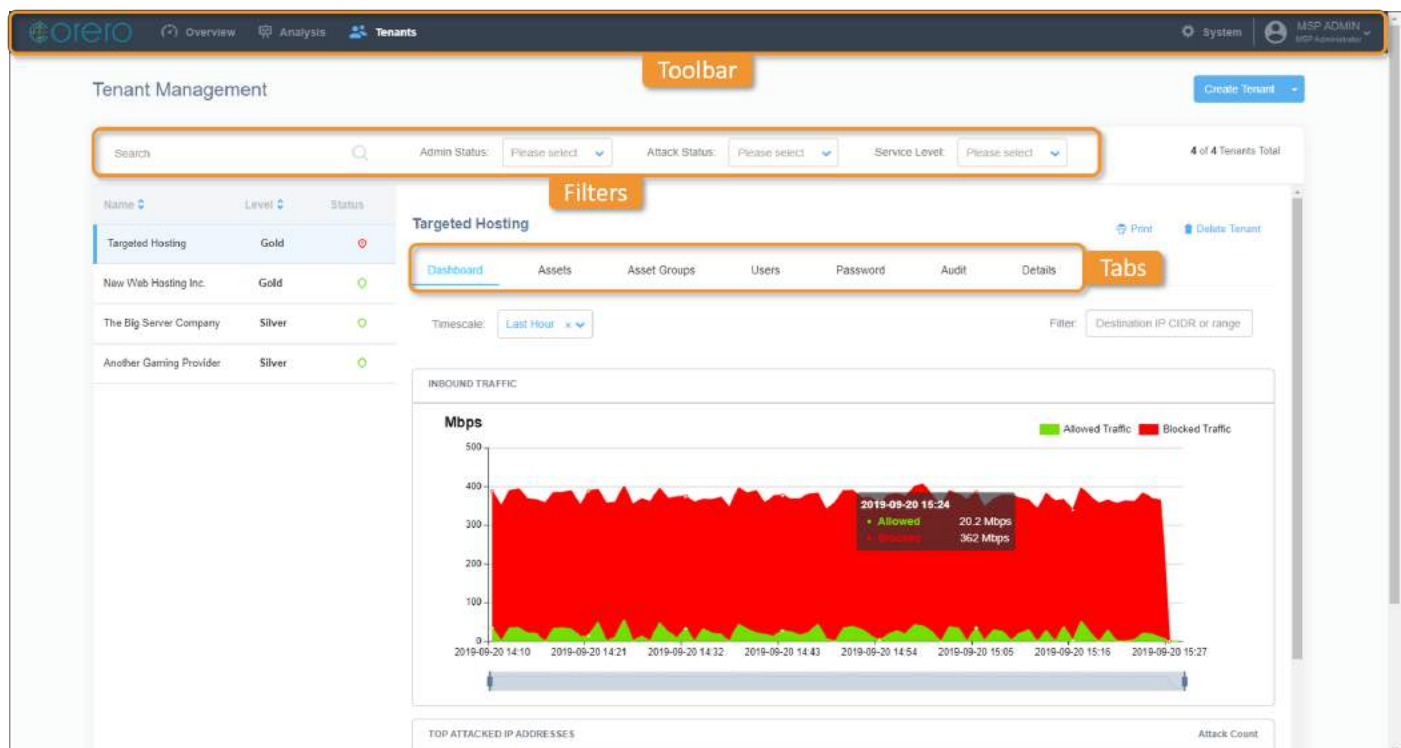
Each tenancy in your Service Portal can have multiple users, each with their own login credentials, with two types of user role available:

- **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 tenant 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.

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 service policy, use the drop-down to select the level this tenant has subscribed to.
 - **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**.
 - **Full Name** – Type the name of the primary contact for this tenant. This name is used when emailing the tenant.
 - **Email** – Type the email address of the primary contact. All email correspondence for the tenant will be directed here. This will also be the tenant's username.
 - **Phone** – (Optional) Type the phone number of the primary contact
 - **Address** – (Optional) Type the address of the primary contact
 - **Country** – (Optional) Type which country the primary contact is based in
4. Click **Save**.

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. Replace the example content with your tenant information 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 session, first click **Tenants > Create Tenant** drop-down to return to the Import dialog.
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.txt file 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), you will see a red error message and none of the tenants will be imported.

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 use the following information to replace the placeholder text:
 - **Tenant1** – Replace the text with the name of a tenant (as you want it to appear in the tenant's portal)
 - **description1** – Replace the text with a description of the tenant (as you want it to appear in the tenant's portal)
 - **MyServicePolicy** – Replace the text with the policy level you want to assign this tenant
 - **ENABLED** – Leave as **ENABLED** to enable your tenant on creation or replace with **DISABLED** to create the tenant as disabled and choose to enable it at a later date
 - **contactName** – Replace the text with the name of the primary contact for the tenant (e.g. "Joseph Bloggs")
 - **email@tenant1.com** – Replace the text with the email address for the primary contact for the tenant (e.g. "j.bloggs@company.com")
 - **contactPhoneNumber** – Replace the text with a phone number for your the primary contact for the tenant (e.g. "+1-541-754-3010")
 - **address** – Replace the text with the address for your the primary contact for the tenant (e.g. "101 Main Street, Marlborough")
 - **United States** – If your tenant is in the US, leave as **United States**. Otherwise replace United States with the country your tenant resides in.
- The tenant information must be in the following order: name, description, policyName, ENABLED, contactName, email@tenant1.com, contactPhoneNumber, address, country
- 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 (,).
- The first row in the example file (#This is a comment) is optional. It is ignored by the Service Portal but you can use it to add a comment about the file for other people using it.

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.
 - **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

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.

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.

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

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.txt 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 created 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
- 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.

Changing a Tenant Name and Description

You can update the tenant's name and description, which appears on the Tenant Management screen and the tenant's Service Overview screen.

To change a tenant's name

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 **Details** tab.
4. Inside the Details tab, edit the **Tenant Name**.
5. Scroll down and click **Save**.

To change a tenant's description

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 **Details** tab.
4. Edit the **Description** field.
5. Scroll down and click **Save**.

Changing a Tenant Service Level

When a tenant first subscribes to the service, or increases or decreases their service level, you will need to reflect that change in the SmartWall Service Portal.

To change a tenant's service level

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 **Details** tab.
4. From the **Service Level** drop-down, select the new service level the tenant has subscribed to.
5. Scroll down and click **Save**.

Editing a Tenant's Primary Contact Information

For every tenant you must have a primary contact whose information is attached to the tenant account.

To edit a tenant's primary contact information

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 **Details** tab.
4. Edit any of the following details:
 - **Name** – Type the name of the primary contact for this tenant.
 - **Email** – Type the email address of the primary contact. This will also be the tenant's username.
 - **Phone** – (Optional) Type the phone number of the primary contact
 - **Address** – (Optional) Type the address of the primary contact
 - **Country** – (Optional) Type which country the primary contact is based in
5. Scroll down and click **Save**.

Enabling/disabling a Tenancy

If you have temporarily stopped providing services for a tenant you might want to disable their tenancy then later enable it.


To enable or disable a tenancy

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 **Details** tab.
4. Next to **Status**, select from:
 - **Enabled** – You can view the tenancy and all enabled tenant user accounts can access the portal
 - **Disabled** – You can still view the tenancy but none of the Tenant Administrators or Users will be able to access the portal
5. Scroll down and click **Save**.

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.

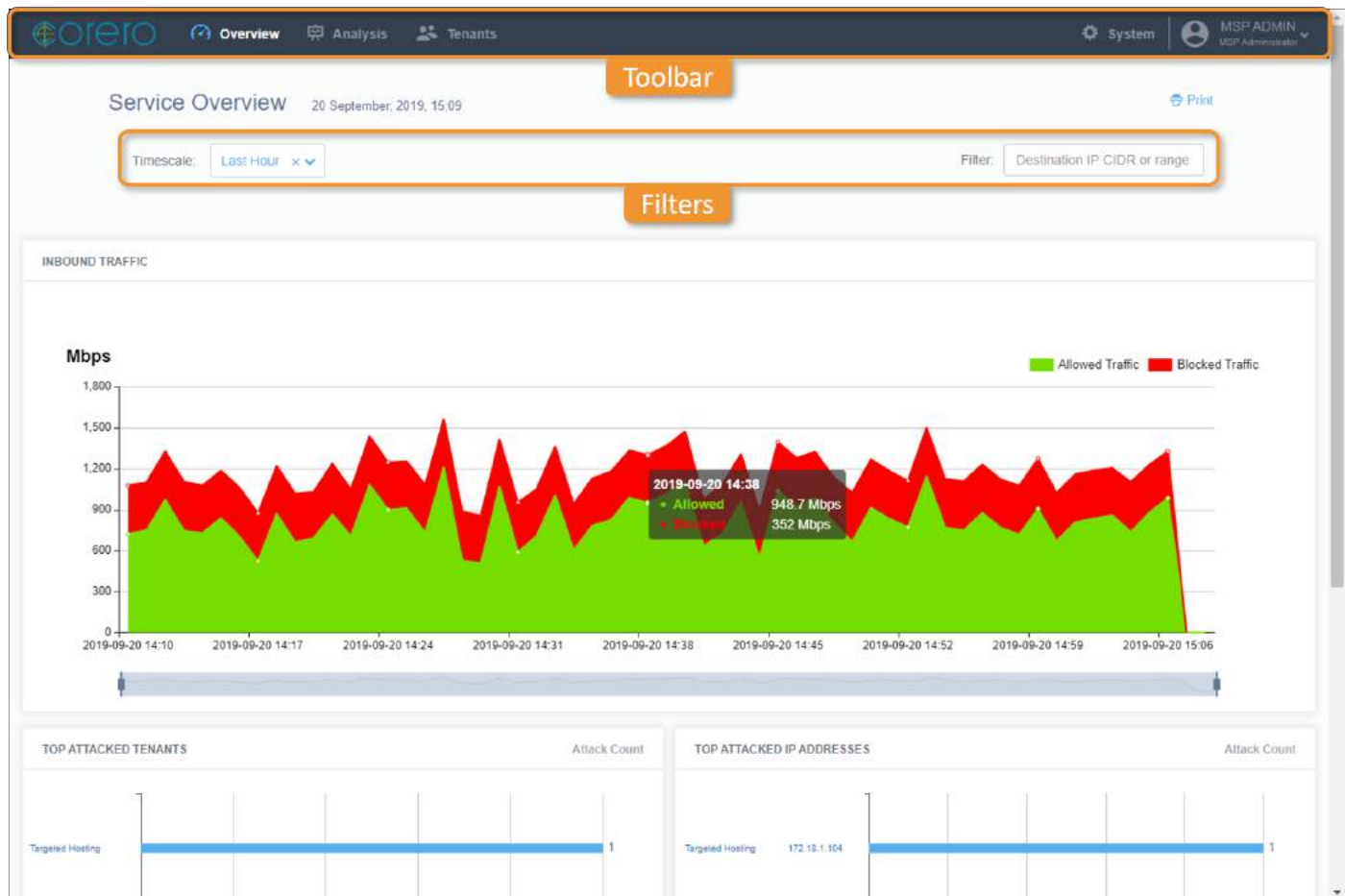
Tip: You can click on a piece of information in a chart in the Overview screen, and the Attack Analysis screen will open showing the data point you clicked in the Overview chart.

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 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.

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

- INBOUND TRAFFIC** chart – Displays the sampled allowed inbound traffic and sampled blocked traffic (in mega-bits per second) for your protected network, over 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 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.

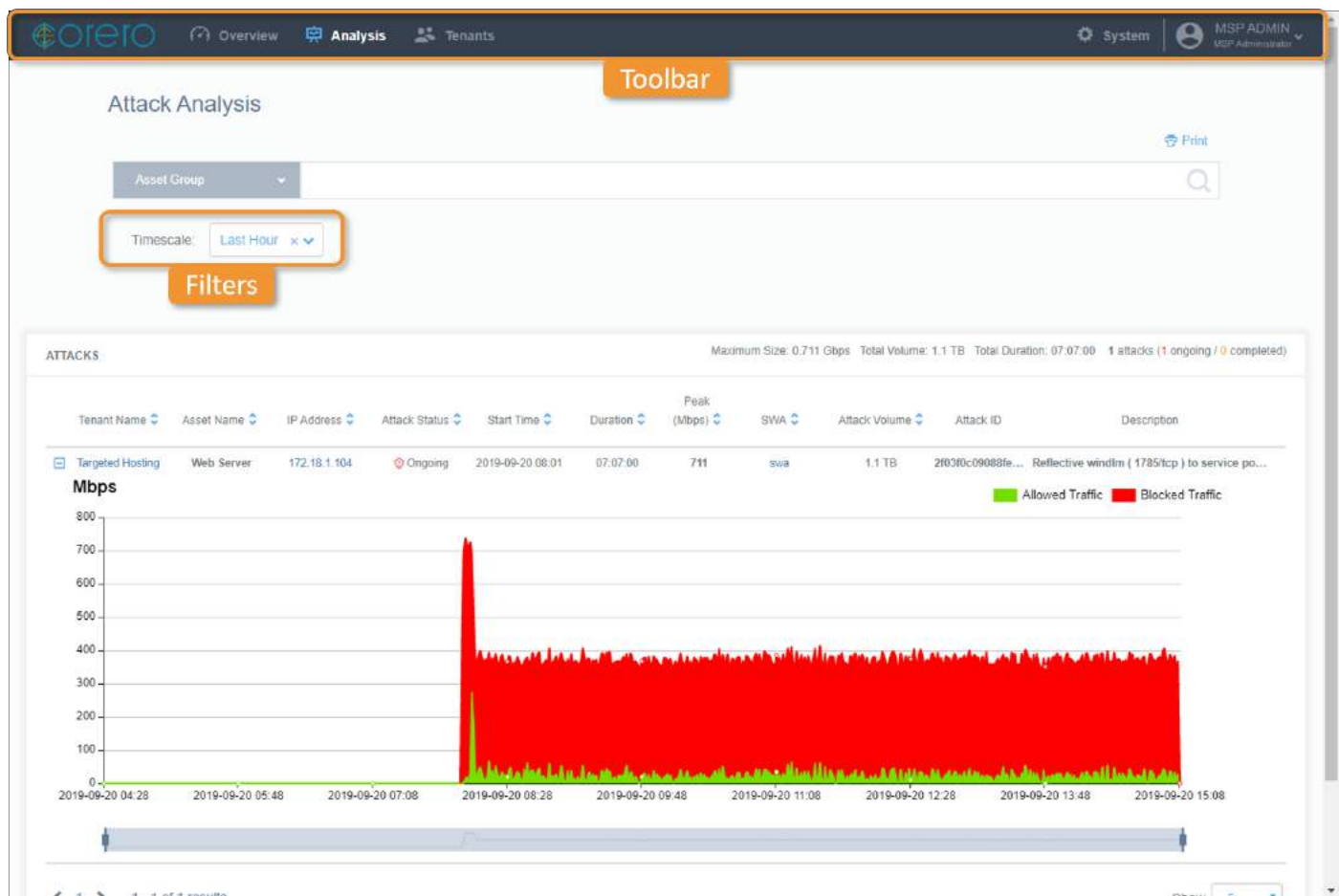
The Attacks table displays the following information for each attack:

- **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 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).
- **Attack Volume** – The volume of traffic sent over the duration of this attack. Only available for SWA 9.7.0 and later, other versions show **n/a**.
- **Description** – A summary of the attack characteristics. If the description is truncated, hover over it to see the full text.

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

Attack Analysis screen

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



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 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. It works in the same way as the [Inbound 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.
- **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 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.

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

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 three Rule Actions, however it provides 3 additional Rule Actions specific to mitigating traffic using edge routers: **Redirect**, **Policer**, and **Ignore**. Traffic affected by Redirect or Ignore Rule Actions are allowed and appear as green on the Service Portal traffic charts. The Policer Rule Action is more flexible and can be used to block or allow traffic. Traffic affected by the Policer Rule Action will therefore appear as either red (blocked) or green (allowed) depending on how that Policer is configured.

Rule Action	SmartWall TDS	SmartWall TDD
Block	Blocked (attack records)	Blocked (attack records)
Detect	Allowed (no attack records)	Allowed (no attack records)
Disabled	Allowed (no attack records)	Allowed (no attack records)
Redirect	n/a	Allowed (no attack records)
Policer	n/a	Blocked or Allowed depending on policer action (no attack records)
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.

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.
7. You will print a report listing all the attacks directed at that IP address over the last week.

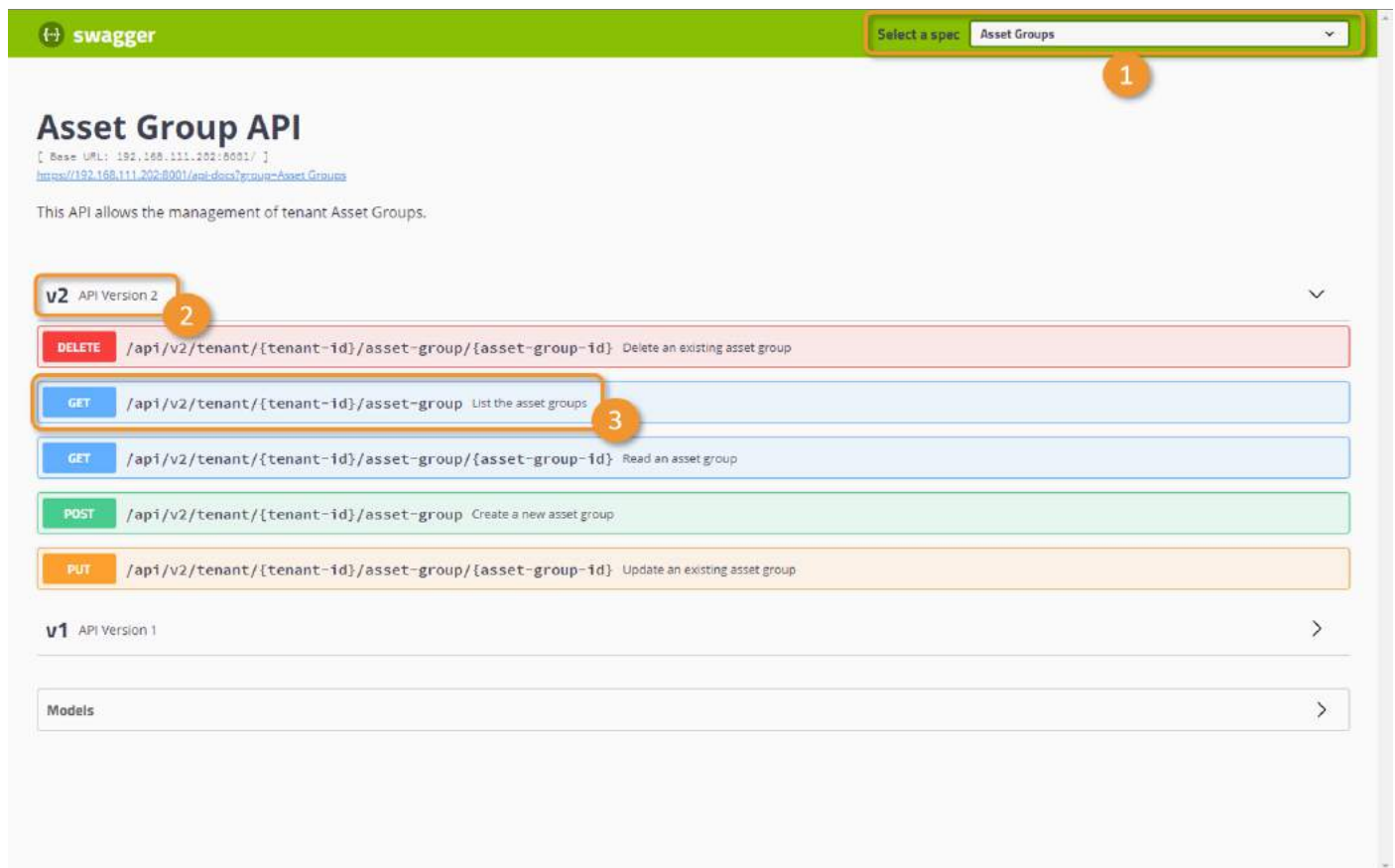
Service Portal REST API Overview

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



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 HTML 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.

HTML return codes

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

Code	Message	Description
200	OK	Your request was completed successfully and a response is returned.

Code	Message	Description
201	Created	Your requested resource was created. The news 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 **v2**.

Tip: You can see operations for v1 and v2 in the Swagger REST API documentation.

Etags

Version 2 of the Service Portal Rest API supports the use of Etags.

Using cURL

One of the simplest ways to send REST commands from outside of Swagger, is using cURL. The only difference, between the suggested cURL commands provided by the Swagger documentation and the commands you need to send, is providing authentication.

For example, the Swagger documentation suggests the following cURL command for getting a list of all tenants (where 10.10.148.87 is the IP of the Service Portal):

```
curl -X GET --header 'Accept: application/json' 'https://10.10.148.87/api/v2/tenant'
```

To use this command outside of the Swagger session, you must add `-u` followed by your administrator access credentials. You can optionally add `-k` if your Service Portal uses a self-signed certificate or the client does not have the correct CA certificate installed..

```
curl -k -u admin@admin.com:Admin123 -X GET --header 'Accept: application/json'
'https://10.10.148.87/api/v2/tenant'
```

Note: You must use `-u` and your credentials on every REST API command you send. Each one is authenticated separately.

cURL Example: Identifying the tenant and service level associated with a DIP

If an attack has happened against a specific IP address in your protected network, you can use the REST API to identify the tenant who has that IP address as part of an Assigned Asset and the service level they currently subscribe to.

Send the following request:

```
curl -k -u admin@admin.com:Admin123 -X GET --header 'Accept: application/json'
'https://<portal_IP>/api/v2/tenant/search?ip=<attacked_IP>'
```

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**.

Appendix: Using a Remote Database

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

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://www.juniper.net/customers/csc/software/>
- 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://www.juniper.net/cm/>

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://myjuniper.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
- Web: <https://corero.force.com/support>
- Telephone: Dial +1.978.212.1500 -> Select Option 2